

# Affine difference algebraic groups

Michael Wibmer

May 27, 2014

## Abstract

We study groups defined by algebraic difference equations. These groups occur as the Galois groups of linear differential and difference equations depending on discrete parameters. Among the main results are three finiteness theorems, the introduction of numerical invariants such as the limit degree, a dimension theorem for difference algebraic groups, an analog of Chevalley's theorem on representations and an analog of the Jordan–Hölder theorem.

## Introduction

The central objects of study in this article are affine difference algebraic groups. Similarly to the case of affine algebraic groups, these groups can all be realized as subgroups of the general linear group defined by algebraic difference equations. The defining equations here are not simply polynomials in the matrix entries but difference polynomials, i.e., the defining equations involve a difference operator  $\sigma$ , which has to be interpreted as a ring endomorphism. For example, if  $G$  is the difference algebraic subgroup of  $\mathrm{GL}_n$  defined by the algebraic difference equations  $X\sigma(X)^T = \sigma(X)^T X = I_n$ , then  $G(\mathbb{C})$  is the group of all complex unitary  $n \times n$ -matrices, where  $\sigma: \mathbb{C} \rightarrow \mathbb{C}$  is the complex conjugation map. A more classical example of a difference field, i.e., a field equipped with an endomorphism would be  $\mathbb{C}(x)$  with  $\sigma(f(x)) = f(x+1)$ .

Alternatively, affine difference algebraic groups may be described as affine group schemes with a certain additional structure (the difference structure). As schemes they are typically not of finite type, but they enjoy a certain finiteness property with respect to the difference structure; they are “of finite  $\sigma$ -type”. From an algebraic point of view, an affine difference algebraic group  $G$  over a difference field  $k$  corresponds to a Hopf algebra  $k\{G\}$  over  $k$  together with a ring endomorphism  $\sigma: k\{G\} \rightarrow k\{G\}$  which extends  $\sigma: k \rightarrow k$ . The Hopf algebra structure maps are required to commute with  $\sigma$ , and  $k\{G\}$  is required to be finitely  $\sigma$ -generated over  $k$ , i.e., there exists a finite set  $B \subset k\{G\}$  such that  $B, \sigma(B), \sigma^2(B), \dots$  generates  $k\{G\}$  as a  $k$ -algebra.

Difference algebraic groups are the discrete analog of differential algebraic groups, i.e., groups defined by algebraic differential equations. Differential algebraic groups have always played an important role in differential algebra (see, e.g., [Cas72], [Sit75], [Cas75], [Cas78], [Kol85], [Cas89] [Bui92], [Bui93]) and are an active area of research nowadays. See e.g., [Pil97], [KP00], [CS11], [MO11], [MO13], [Fre], [Min]. See also [Mal10] for a more geometric approach to differential algebraic groups and [Bui98] for an arithmetic analog of difference/differential algebraic groups.

Over the last decade, Galois theories where the Galois groups are differential algebraic groups ([Pil98], [Lan08], [CS07], [HS08]) have given a new impetus to the study of differential algebraic groups. The Galois theories in [CS07] and [HS08] are also known as parameterized Picard–Vessiot theories as they generalize the standard Picard–Vessiot theory ([Kol48], [vdPS03], [vdPS97]) of linear differential and difference equations to linear differential and difference equations depending on (continuous) parameters. In the standard Picard–Vessiot theory the Galois groups are linear algebraic groups and they measure the algebraic dependencies among the solutions. In the parameterized Picard–Vessiot theory the Galois groups are linear differential algebraic groups and they measure the differential algebraic dependencies with respect to an auxiliary set of derivations. A typical application of the parameterized Picard–Vessiot theory is to prove the differential transcendence of special functions ([Arr13], [DV12]).

The tannakian approach to differential algebraic groups ([Ovc08]) has found applications in the parameterized Galois theory ([Ovc09], [GG013], [GA]) and a detailed study of representations of linear differential algebraic groups has led to the first algorithms for computing the Galois group of parameterized linear differential equations ([MOSb], [MOSa], [Arr], [Dre14]).

In contrast to the situation in differential algebra, difference algebraic groups have long played no role at all in difference algebra. The author can only speculate why. Maybe because the traditional definition of a difference variety, which involves a so-called universal system of difference fields (see [Coh65, Chapter 4]) is not really suitable for studying groups. (For each difference field in the universal system one obtains a group structure but the difference variety itself does not carry a group structure.)

Around the turn of the century a considerable interest in the model theory of difference fields emerged. (See e.g., [Mac97], [CH99], [CHP02].) Groups definable in ACFA, the model companion of the theory of difference fields, played a crucial role in remarkable applications of model theory to number theory, especially regarding the Manin–Mumford conjecture. See [Hru01], [Bou02], [Cha01], [Cha97], [Sca05], [Sca06], [SV99], [KP07].

In [KP02] it is shown that every group definable in ACFA is, in a certain sense, close to being a definable (in the language of difference fields) subgroup of an algebraic group. Here we will show that every affine difference algebraic group is isomorphic to a difference closed subgroup of the general linear group. In [KP02] it is also shown that an affine difference algebraic group whose underlying difference variety is an affine space is isomorphic to a difference closed subgroup of a unipotent algebraic group.

Recently, a Galois theory for linear differential equations depending on a discrete parameter has been developed in [DVHW14]. In [OWa] a similar Galois theory has been developed for linear difference equations depending on a discrete parameter. The Galois groups in these Galois theories are affine difference algebraic groups and they measure the difference algebraic relations among the solutions. For example, the difference algebraic relation  $xJ_{\alpha+2}(x) - 2(\alpha+1)J_{\alpha+1}(x) + xJ_{\alpha}(x) = 0$  satisfied by the Bessel function  $J_{\alpha}(x)$ , which solves Bessel's differential equation  $x^2\delta^2(y) + x\delta(y) + (x - \alpha^2)y = 0$ , is witnessed by the associated Galois group.

As illustrated in [DVHW] and [OWa], these Galois theories make it possible to use structure results about affine difference algebraic groups to analyze and classify the possible difference algebraic relations among the solutions of certain linear differential and difference equations. In this respect the understanding of the Zariski dense difference closed subgroups of a given affine algebraic group is highly relevant. For example, some understanding of the Zariski dense difference closed subgroups of  $SL_2$ , originating from [CHP02], is a key ingredient to prove that any two linearly independent solutions of the Airy equation are difference algebraically independent. More precisely ([DVHW, Corollary 6.10]), if  $A(x)$  and  $B(x)$  are  $\mathbb{C}$ -linearly independent solutions of Airy's equation  $\delta^2(y) - xy = 0$ , then  $A(x), B(x), A'(x), A(x+1), B(x+1), A'(x+1), A(x+2), \dots$  are algebraically independent over  $\mathbb{C}(x)$ .

While the parameterized Picard–Vessiot theory for continuous parameters could draw on a well-established comprehensive theory of differential algebraic groups, the situation for discrete parameters is adverse. But clearly, a well-developed theory of affine difference algebraic groups is indispensable for the parameterized Picard–Vessiot theory with discrete parameters to flourish. Obviously one could not get very far without having fundamental results such as the analogs of the isomorphism theorems for groups at one's disposal. Even though the validity of the isomorphism theorems for affine difference algebraic may not come as a surprise, the proof is far from being obvious. Indeed, even the existence of the quotient of an affine difference algebraic group modulo a normal difference closed subgroup is a highly non-trivial question. A positive answer requires proving that every  $k$ - $\sigma$ -Hopf subalgebra of a finitely  $\sigma$ -generated  $k$ - $\sigma$ -Hopf algebra is finitely  $\sigma$ -generated.

While it will for sure be a long way to lift the theory of difference algebraic groups to a level comparable to the contemporary theory of differential algebraic groups, it is the hope of the author that this article may serve as a first step in this direction. Here we are mainly concerned with general properties of affine difference algebraic groups. We plan to study special classes (e.g., étale, unipotent, diagonalizable) affine difference algebraic groups next.

A tannakian approach to affine difference algebraic groups has been developed in [OWb]. (See also [Kam13].) We expect that the finiteness properties of affine difference algebraic groups proved here will enable us to apply this tannakian approach to the parameterized Picard–Vessiot theory with discrete parameters in a similar fashion as for the case of continuous parameters in [GGO13].

It is well recognized that a functorial–schematic approach to algebraic groups has its benefits. (See [Wat79], [DG70], [Jan87], [Mil12], [Gro70].) Here we adopt a similar approach for difference algebraic groups. For example, the general linear group  $GL_n$  over a difference field  $k$ , considered as a difference algebraic group, is the functor which assigns  $GL_n(R)$  to every  $k$ - $\sigma$ -algebra  $R$ , that is,  $R$  is a  $k$ -algebra equipped with an endomorphism  $\sigma: R \rightarrow R$  which extends  $\sigma: k \rightarrow k$ . In the model theoretic approach to difference equations as well as in classical difference algebra ([Coh65], [Lev08]) one is primarily interested in solutions in difference field extensions of  $k$ , i.e.,  $R$  is required to be a field. An affine difference algebraic

group is a group object in the category of affine difference varieties. The definition of an affine difference variety used in this article is more general than the classical definition of a difference variety (as in [Coh65] and [Lev08]). Our definition is equivalent to what is called a  $\underline{\mathcal{D}}$ -subscheme of affine space in [MS11] for a suitable choice of  $\underline{\mathcal{D}}$ . Also, our notion of affine difference algebraic group is equivalent to what is called a linear  $\mathfrak{M}$ -group in [Kam13] for a suitable choice of  $\mathfrak{M}$ . The classical difference varieties studied in [Coh65] and [Lev08] correspond precisely to the affine difference varieties which can be recovered from their points in difference fields. Thus, the relation between our affine difference varieties and the classical difference varieties is similar to the relation between affine schemes of finite type and affine varieties. The affine difference varieties which can be recovered from their points in difference fields are those whose defining ideal is perfect, therefore, we call them perfectly  $\sigma$ -reduced. Affine difference algebraic groups which are not perfectly  $\sigma$ -reduced occur quite naturally and frequently as Galois groups of linear differential or difference equations depending on a discrete parameter. There are several examples (Example 9.2) of difference algebraic groups  $G$  with the property that  $G(K)$  is the trivial group for every difference field extension  $K$  of  $k$ .

In difference algebraic geometry there is a “zoo” of elements playing a role analogous to nilpotent elements in algebraic geometry. They roughly correspond to the following assertions valid for elements in a difference field extension of  $k$  but not necessarily valid for elements in a  $k$ - $\sigma$ -algebra:

- $a^n = 0$  implies  $a = 0$ .
- $\sigma^n(a) = 0$  implies  $a = 0$ .
- $ab = 0$  implies  $a\sigma(b) = 0$ .
- $a\sigma(a) = 0$  implies  $a = 0$ .

In this sense we obtain four difference closed subgroups of an affine difference algebraic group which play a role analogous to the maximal reduced subgroup of an affine algebraic group. The theory of affine algebraic groups runs smoother if one allows nilpotent elements in the structure sheaf, and non-reduced algebraic groups play an important role in the representation theory of affine algebraic groups in positive characteristic. The situation for affine difference algebraic groups is similar. The category of affine difference algebraic groups is much better behaved than the category of perfectly  $\sigma$ -reduced affine difference algebraic groups. This, for example, becomes apparent when dealing with extensions of the base field or when dealing with quotients and the analogs of the isomorphism theorems for groups. For example, the morphism of affine difference algebraic groups  $\phi: \mathrm{GL}_n \rightarrow \mathrm{GL}_n$  determined by  $\phi((g_{ij})) = (\sigma(g_{ij}))$  for  $(g_{ij}) \in \mathrm{GL}_n(R)$  and  $R$  a  $k$ - $\sigma$ -algebra has a non-trivial kernel, even though  $\phi: \mathrm{GL}_n(K) \rightarrow \mathrm{GL}_n(K)$  is injective for every difference field extension of  $k$ . In particular, if  $k$  is a model of ACFA, then  $\phi: \mathrm{GL}_n(k) \rightarrow \mathrm{GL}_n(k)$  is bijective but  $\phi$  is not an isomorphism of difference algebraic groups. Here we will show that (with the appropriate conception of injective and surjective) a morphism of affine difference algebraic groups is an isomorphism if and only if it is injective and surjective.

Even though our notion of an affine difference algebraic group as well as the notion of a group definable in ACFA both capture the idea of a group defined by algebraic difference equations, there are several differences between the two notions. On the one hand groups definable in ACFA are more general since they need not be affine, for example [CH] studies definable subgroups of semi-abelian varieties. Moreover, since ACFA does not (fully) eliminate quantifiers, a group definable in ACFA may not be definable by difference polynomials. For example, the formula  $\exists h : h^2 = g, \sigma(h) = h$  defines a subgroup of the multiplicative group and the existential quantifier can not be eliminated.

On the other hand, if  $k$  is a model of ACFA, the subgroups of  $\mathrm{GL}_n(k)$  defined by difference polynomials in the matrix entries only correspond to the perfectly  $\sigma$ -reduced difference closed subgroups of  $\mathrm{GL}_n$ .

Let  $k$  be a difference field and  $K$  a model of ACFA containing  $k$ . Unfortunately, the functor which associates to a perfectly  $\sigma$ -reduced affine difference algebraic  $G$  over  $k$  its  $K$ -points  $G(K)$  is not faithful, as the embedding  $k \hookrightarrow K$  involves a non-canonical choice. For example, if  $k = \mathbb{Q}$  and  $G$  is the difference closed subgroup of the multiplicative group given by  $G(R) = \{g \in R^\times \mid g^3 = 1, \sigma(g) = g\}$  for any  $k$ - $\sigma$ -algebra  $R$ , then  $G$  has a non-trivial endomorphism given by  $g \mapsto g^2$ . But if  $K$  is a model of ACFA of characteristic zero such that  $\sigma$  permutes the two non-trivial third roots of unity in  $K$ , then  $G(K)$  is the trivial group and the endomorphism of  $G$  collapses to the identity on  $G(K)$ . To obtain a faithful functor, one would need to impose restrictions on the base difference field  $k$ , but this is something we wish to avoid as it would reduce the applicability of the theory.

Let us now describe the content of the article in more detail. The first section contains preliminaries from difference algebraic geometry. We introduce affine difference varieties and some basic constructions with them. In the second section we define affine difference algebraic groups, present several examples and show that every affine difference algebraic group is isomorphic to a difference closed subgroup of the general linear group. In particular, an affine difference algebraic group  $G$  can be embedded into an algebraic group (as a difference closed subgroup). In Section 3 we explain how to associate to any such embedding an affine algebraic group called the growth group. We also prove the existence of a Kolchin (or dimension) polynomial for affine difference algebraic groups and define the difference dimension and the order of an affine difference algebraic group. While the growth group depends on the chosen embedding, we will show that it contains some information which only depends on  $G$ . For example, its dimension is equal to the difference dimension of  $G$ .

In Section 4 we prove two important finiteness theorems. For clarity we state here the theorems in the language of Hopf algebras: Let  $k\{G\}$  be a  $k$ - $\sigma$ -Hopf algebra which is finitely  $\sigma$ -generated over  $k$  and let  $\mathbb{I}(H) \subset k\{G\}$  be a  $\sigma$ -Hopf ideal, i.e., a Hopf ideal such that  $\sigma(\mathbb{I}(H)) \subset \mathbb{I}(H)$ . Then  $\mathbb{I}(H)$  is finitely  $\sigma$ -generated, i.e., there exists a finite set  $B \subset \mathbb{I}(H)$  such that  $B, \sigma(B), \sigma^2(B), \dots$  generates  $\mathbb{I}(H)$  as an ideal. This result can be seen as a strengthening (for  $k$ - $\sigma$ -Hopf algebras) of the Ritt–Raudenbush basis theorem in difference algebra. The classical Ritt–Raudenbush basis theorem does not apply in our setting as it only applies to perfect difference ideals. This finiteness result turns out to be extremely useful and is used repeatedly in the subsequent developments. For example, it is used in the proof of the dimension theorem which is also proved in Section 4. The second finiteness theorem asserts that every  $k$ - $\sigma$ -Hopf subalgebra of  $k\{G\}$  is finitely  $\sigma$ -generated.

In Section 5 we briefly touch upon representations of affine difference algebraic groups. The main result here is an analog of a theorem of Chevalley: Every difference closed subgroup of  $G$  is the stabilizer of a line in a suitable representation of  $G$ . We also show that the category of representations of a torus (considered as a difference algebraic group) is semi-simple. This is in sharp contrast to what happens in the theory of linear differential algebraic groups. The category of representations of a linear differential algebraic group is semi-simple only for linear differential algebraic groups which are the constant points of a reductive algebraic group ([MO11]).

In Section 6 we introduce a numerical invariant of affine difference algebraic groups called the limit degree. Its definition is analogous to an important invariant of extensions of difference fields also called the limit degree ([Lev08, Section 4.3]). So-called algebraic  $\sigma$ -groups have been introduced and studied in [KP07]. We show that the category of affine algebraic  $\sigma$ -groups is equivalent to the category of affine difference algebraic groups of difference dimension zero and limit degree one.

In Section 7 we establish the existence of quotients and show that the difference dimension, the order and the limit degree behave on quotient in the expectable way.

Section 8 then studies morphisms of affine difference algebraic groups. We characterize injective and surjective morphisms and show that every morphism of affine difference algebraic groups factors uniquely as the composition of a surjective morphism followed by an injective morphism.

In Section 9 we study the components of affine difference algebraic groups. We introduce the connected component and prove a third finiteness theorem: A finitely  $\sigma$ -generated  $k$ - $\sigma$ -Hopf algebra has only finitely many minimal prime difference ideals. This proves a special case of a reformulation of a question raised by E. Hrushovski.

In Section 10 we deal with the ring elements playing a role analogous to nilpotent elements in algebraic geometry. In particular, we introduce four difference closed subgroups playing a role analogous to the maximal reduced subgroup for algebraic groups.

Sheaves ([DG70, Chapter III]) are a useful tool for dealing with quotients of algebraic groups. In Section 11 we adapt the sheaf approach to difference algebraic groups and then use it to prove the analogs of the isomorphism theorems for groups.

Section 12 then further expands on the group theoretic properties of affine difference algebraic groups. We prove an analog of the Jordan–Hölder decomposition theorem.

Finally, in Section 13 we present an application to the parameterized Picard–Vessiot theory with discrete parameters.

# 1 Difference algebraic geometry preliminaries

In this section we introduce some basic notions from difference algebraic geometry, e.g., the notion of a difference variety. These definitions and results will then be used in the following sections in the study of difference algebraic groups.

## 1.1 Basic definitions

We start by recalling some basic notions from difference algebra. Standard references are [Lev08] and [Coh65]. All rings are assumed to be commutative and unital.

A difference ring, or  $\sigma$ -ring for short, is a ring  $R$  together with a ring endomorphism  $\sigma: R \rightarrow R$ . Contrary to [Lev08] we do not assume that  $\sigma: R \rightarrow R$  is injective. If  $R$  is a field, we speak of a  $\sigma$ -field. We usually omit  $\sigma$  from the notation, and simply refer to  $R$  as a  $\sigma$ -ring. A morphism between  $\sigma$ -rings  $R$  and  $S$  is a morphism  $\psi: R \rightarrow S$  of rings such that  $\psi(\sigma(r)) = \sigma(\psi(r))$  for all  $r \in R$ . A  $\sigma$ -ring  $R$  is called *inversive* if  $\sigma: R \rightarrow R$  is an automorphism. A subset  $A$  of a  $\sigma$ -ring  $R$  is called *stable under  $\sigma$*  if  $\sigma(A) \subset A$ .

Let  $k$  be a  $\sigma$ -ring. A  $\sigma$ -ring  $R$  together with a  $k$ -algebra structure is called a  $k$ - $\sigma$ -algebra if the algebra structure map  $k \rightarrow R$  is a morphism of  $\sigma$ -rings. A morphism of  $k$ - $\sigma$ -algebras is a morphism of  $k$ -algebras which is also a morphism of  $\sigma$ -rings. The category of  $k$ - $\sigma$ -algebras is denoted by  $k$ - $\sigma$ -Alg. A  $k$ -subalgebra of a  $k$ - $\sigma$ -algebra is called a  $k$ - $\sigma$ -subalgebra if it is stable under  $\sigma$ . If  $k$  is a  $\sigma$ -field, a  $k$ - $\sigma$ -algebra which is a  $\sigma$ -field is called a  $\sigma$ -field extension of  $k$ .

Let  $R$  and  $S$  be  $k$ - $\sigma$ -algebras. Then  $R \otimes_k S$  is naturally a  $k$ - $\sigma$ -algebra by  $\sigma(r \otimes s) = \sigma(r) \otimes \sigma(s)$  for  $r \in R$  and  $s \in S$ .

Let  $k$  be a  $\sigma$ -field and  $R$  a  $k$ - $\sigma$ -algebra. For a subset  $A$  of  $R$ , the smallest  $k$ - $\sigma$ -subalgebra of  $R$  containing  $A$  is denoted by  $k\{A\}$ . If there exists a finite subset  $A$  of  $R$  such that  $R = k\{A\}$ , we say that  $R$  is finitely  $\sigma$ -generated over  $k$ .

The  $\sigma$ -polynomial ring over  $k$  in the  $\sigma$ -variables  $y = (y_1, \dots, y_n)$  is the polynomial ring over  $k$  in the variables  $y_1, \dots, y_n, \sigma(y_1), \dots, \sigma(y_n), \sigma^2(y_1), \dots$ . It is denoted by

$$k\{y\} = k\{y_1, \dots, y_n\}$$

and has a natural  $k$ - $\sigma$ -algebra structure.

If  $R$  is a  $k$ - $\sigma$ -algebra and  $F \subset k\{y\}$  a set of  $\sigma$ -polynomials over  $k$ , it makes sense to consider the  $R$ -rational solutions of  $F$ , that is

$$\mathbb{V}_R(F) = \{a \in R^n \mid f(a) = 0 \text{ for all } f \in F\}.$$

Note that  $R \rightsquigarrow \mathbb{V}_R(F)$  is naturally a functor from  $k$ - $\sigma$ -Alg to **Sets**, the category of sets. We denote this functor by  $\mathbb{V}(F)$ .

**Definition 1.1.** Let  $k$  be a  $\sigma$ -field. A difference variety (or  $\sigma$ -variety for short) over  $k$  is a functor from  $k$ - $\sigma$ -Alg to **Sets**, which is of the form  $\mathbb{V}(F)$ , for some  $n \geq 1$  and  $F \subset k\{y_1, \dots, y_n\}$ . A morphism of  $\sigma$ -varieties is a morphism of functors.

The above definition does not agree with the traditional definition of a difference variety in [Lev08], since traditionally one is only interested in solutions in  $\sigma$ -field extensions of  $k$ . The relation between Definition 1.1 and Definition 2.6.1 in [Lev08] is analogous to the relation between the definition of an affine scheme of finite type over a field and the notion of an affine variety. Our definition is equivalent to what is called a  $\underline{D}$ -subscheme of affine space in [MS11] for a suitable choice of  $\underline{D}$ . It may seem more accurate to add the word “affine” into Definition 1.1. However, to avoid endless iterations of the word “affine” we have chosen not to do so.

By definition, a morphism  $\phi: X \rightarrow Y$  of  $\sigma$ -varieties consists of maps  $\phi_R: X(R) \rightarrow Y(R)$  for any  $k$ - $\sigma$ -algebra  $R$ . For convenience, we will sometimes drop the  $R$  in  $\phi_R$ . In particular, if  $x \in X(R)$ , we may write  $\phi(x)$  for  $\phi_R(x) \in Y(R)$ .

Let  $F, G \subset k\{y\}$  and  $X = \mathbb{V}(F)$ ,  $Y = \mathbb{V}(G)$ . If  $F \subset G$  then  $Y(R) \subset X(R)$  for every  $k$ - $\sigma$ -algebra  $R$  and  $Y$  is a subfunctor of  $X$ . We say that  $Y$  is a  $\sigma$ -closed  $\sigma$ -subvariety of  $X$  and write  $Y \subset X$ .

Let  $R$  be a  $\sigma$ -ring. An ideal  $\mathfrak{a}$  of  $R$  is called a  $\sigma$ -ideal if  $\sigma(\mathfrak{a}) \subset \mathfrak{a}$ . In this case  $R/\mathfrak{a}$  has naturally the structure of a  $\sigma$ -ring such that the canonical map  $R \rightarrow R/\mathfrak{a}$  is a morphism of  $\sigma$ -rings. If  $A$  is a subset of  $R$ , the smallest  $\sigma$ -ideal of  $R$  containing  $A$  is denoted by

$$[A] \subset R$$

and called the  $\sigma$ -ideal generated by  $A$ . A  $\sigma$ -ideal  $\mathfrak{a} \subset R$  is *finitely generated as a  $\sigma$ -ideal* if there exists a finite set  $A \subset \mathfrak{a}$  such that  $\mathfrak{a} = [A]$ . A  $\sigma$ -ideal  $\mathfrak{p}$  of  $R$  which is a prime ideal is called  *$\sigma$ -prime* if  $\sigma^{-1}(\mathfrak{p}) = \mathfrak{p}$ .

Let  $X = \mathbb{V}(F)$ ,  $F \subset k\{y\} = k\{y_1, \dots, y_n\}$  be a  $\sigma$ -variety over the  $\sigma$ -field  $k$ . Then

$$\mathbb{I}(X) = \{f \in k\{y\} \mid f(a) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } a \in X(R)\} \quad (1)$$

is a  $\sigma$ -ideal of  $k\{y\}$ . The  $k$ - $\sigma$ -algebra

$$k\{X\} = k\{y\}/\mathbb{I}(X)$$

is called the *coordinate ring* of  $X$ . As we may choose  $R = k\{y\}/[F]$  in (1), we see that  $\mathbb{I}(X) = [F] \subset k\{y\}$ .

Let  $R$  be  $k$ - $\sigma$ -algebra. The bijection

$$\text{Hom}(k\{X\}, R) \rightarrow X(R)$$

which maps a morphism  $\psi: k\{X\} \rightarrow R$  of  $k$ - $\sigma$ -algebras to  $\psi(\bar{y})$  is functorial in  $R$ . Thus the functor  $X$  is represented by  $k\{X\}$ . Conversely, since every finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra can be written in the form  $k\{y\}/[F]$ , we see that a functor from  $k$ - $\sigma$ -Alg to Sets which is representable by a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra is isomorphic (as a functor) to a  $\sigma$ -variety.

In the sequel we will allow ourselves the little abuse of notation to also call a functor isomorphic to a  $\sigma$ -variety a  $\sigma$ -variety. In particular, we will often identify  $X$  with the functor  $\text{Hom}(k\{X\}, -)$ . Thus a functor  $X$  from  $k$ - $\sigma$ -Alg to Sets is a  $\sigma$ -variety if and only if it is representable by a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra  $k\{X\}$ . It is then clear from the Yoneda lemma that:

**Remark 1.2.** *The category of  $\sigma$ -varieties over  $k$  is anti-equivalent to the category of finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebras.*

If  $\phi: X \rightarrow Y$  is a morphism of  $\sigma$ -varieties over  $k$ , the dual morphism of  $k$ - $\sigma$ -algebras is denoted by

$$\phi^*: k\{Y\} \rightarrow k\{X\}.$$

Let  $R$  and  $S$  be  $k$ - $\sigma$ -algebras. Then  $R \otimes_k S$  is a  $k$ - $\sigma$ -algebra by  $\sigma(r \otimes s) = \sigma(r) \otimes \sigma(s)$ . Obviously  $R \otimes_k S$  is the coproduct of  $R$  and  $S$  in the category of  $k$ - $\sigma$ -algebras. From this it follows immediately that:

**Remark 1.3.** *The category of  $\sigma$ -varieties has products. Indeed, if  $X$  and  $Y$  are  $\sigma$ -varieties over  $k$ , then  $k\{X \times Y\} = k\{X\} \otimes_k k\{Y\}$ . Moreover, there is a terminal object, namely, the functor represented by the  $k$ - $\sigma$ -algebra  $k$ .*

## 1.2 Difference subvarieties and morphisms of difference varieties

Let  $Y$  be a  $\sigma$ -variety and  $f \in k\{Y\}$ . Then, for any  $k$ - $\sigma$ -algebra  $R$ , we have a well-defined map  $f: Y(R) \rightarrow R$  given by evaluating a representative of  $f$  in  $k\{y_1, \dots, y_n\}$  at  $a \in Y(R) \subset R^n$ . In a coordinate free manner  $f: Y(R) \rightarrow R$  can be described as the map that sends  $\psi \in Y(R) = \text{Hom}(k\{Y\}, R)$  to  $\psi(f) \in R$ .

Let  $X$  be a  $\sigma$ -closed  $\sigma$ -subvariety of  $Y$ . Then

$$\mathbb{I}(X) = \{f \in k\{Y\} \mid f(a) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } a \in X(R)\} \quad (2)$$

is a  $\sigma$ -ideal of  $k\{Y\}$ . We call  $\mathbb{I}(X) \subset k\{Y\}$  the *defining ideal of  $X$*  (in  $k\{Y\}$ ). This notation is consistent with (1) in the sense that  $\mathbb{I}(X)$  as defined in (1) is the defining ideal of  $X$  in  $k\{y\} = k\{y_1, \dots, y_n\}$ . Moreover,  $\mathbb{I}(X) \subset k\{Y\}$  agrees with the image in  $k\{Y\} = k\{y\}/\mathbb{I}(Y)$  of the defining ideal of  $X$  in  $k\{y\}$ . So  $k\{X\} = k\{Y\}/\mathbb{I}(X)$ .

Conversely, let  $\mathfrak{a} \subset k\{Y\}$  be a  $\sigma$ -ideal. Then we can define a  $\sigma$ -closed  $\sigma$ -subvariety  $\mathbb{V}(\mathfrak{a})$  of  $Y$  by

$$\mathbb{V}(\mathfrak{a})(R) = \{a \in Y(R) \mid f(a) = 0 \text{ for all } f \in \mathfrak{a}\}$$

for any  $k$ - $\sigma$ -algebra  $R$ .

**Lemma 1.4.** *Let  $Y$  be a  $\sigma$ -variety. Then  $\mathbb{I}$  and  $\mathbb{V}$  are mutually inverse bijections between the set of  $\sigma$ -closed  $\sigma$ -subvarieties of  $Y$  and the set of  $\sigma$ -ideals of  $k\{Y\}$ .*

*Proof.* Let  $\mathfrak{a}$  be a  $\sigma$ -ideal of  $k\{Y\}$ . Clearly  $\mathfrak{a} \subset \mathbb{I}(\mathbb{V}(\mathfrak{a}))$ . Since we may choose  $R = k\{Y\}/\mathfrak{a}$  in (2) it follows that  $\mathfrak{a} = \mathbb{I}(\mathbb{V}(\mathfrak{a}))$ .

Let  $X$  be  $\sigma$ -closed  $\sigma$ -subvariety of  $Y$ . Then  $X = \mathbb{V}(\mathfrak{a})$  for some  $\sigma$ -ideal  $\mathfrak{a}$  of  $k\{Y\}$ . So  $\mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(\mathbb{I}(\mathbb{V}(\mathfrak{a}))) = \mathbb{V}(\mathfrak{a}) = X$ .  $\square$

Note that if  $X$  is a  $\sigma$ -closed  $\sigma$ -subvariety of  $Y$  and  $R$  a  $k$ - $\sigma$ -algebra, then  $X(R) \subset Y(R)$  corresponds to  $\{\psi \in \text{Hom}(k\{Y\}, R) \mid \mathbb{I}(X) \subset \ker(\psi)\} \subset \text{Hom}(k\{Y\}, R)$ .

If  $Y$  and  $Z$  are  $\sigma$ -closed  $\sigma$ -subvarieties of a  $\sigma$ -variety  $X$ , then we can define a subfunctor

$$Y \cap Z$$

of  $X$  by  $R \rightsquigarrow Y(R) \cap Z(R)$ . Then  $Y \cap Z$  is a  $\sigma$ -closed  $\sigma$ -subvariety of  $X$ , indeed,  $\mathbb{I}(Y \cap Z) \subset k\{X\}$  is the ideal generated by  $\mathbb{I}(Y)$  and  $\mathbb{I}(Z)$ .

If  $\phi: X \rightarrow Y$  is a morphism of  $\sigma$ -varieties and  $Z \subset Y$  a  $\sigma$ -closed  $\sigma$ -subvariety, we can define a subfunctor

$$\phi^{-1}(Z)$$

of  $X$  by  $R \rightsquigarrow \phi_R^{-1}(Z(R))$ . If  $Z = \mathbb{V}(\mathfrak{a})$  with  $\mathfrak{a} \subset k\{Y\}$ , then

$$\begin{aligned} \phi^{-1}(Z)(R) &= \{\psi \in \text{Hom}(k\{X\}, R) \mid \mathfrak{a} \subset \ker(\psi\phi^*)\} \\ &= \{\psi \in \text{Hom}(k\{X\}, R) \mid \phi^*(\mathfrak{a}) \subset \ker(\psi)\} = \mathbb{V}(\phi^*(\mathfrak{a}))(R). \end{aligned}$$

Therefore  $\phi^{-1}(Z) = \mathbb{V}(\phi^*(\mathfrak{a}))$  is a  $\sigma$ -closed  $\sigma$ -subvariety of  $X$ .

If  $\phi: X \rightarrow Y$  is a morphism of  $\sigma$ -varieties, we can define a subfunctor

$$\text{Im}(\phi)$$

of  $Y$  by  $\text{Im}(\phi)(R) = \phi_R(X(R))$  for any  $k$ - $\sigma$ -algebra  $R$ . In general,  $\text{Im}(\phi)$  will not be a  $\sigma$ -closed  $\sigma$ -subvariety of  $Y$ . It is therefore sometimes helpful to use the following notion, analogous to the scheme theoretic image ([Sta14, Tag 01R5]).

**Lemma 1.5.** *Let  $\phi: X \rightarrow Y$  be a morphism of  $\sigma$ -varieties. There exists a unique  $\sigma$ -closed  $\sigma$ -subvariety*

$$\phi(X)$$

*of  $Y$  with the following property. The morphism  $\phi$  factors through  $\phi(X)$  and if  $Z \subset Y$  is a  $\sigma$ -closed  $\sigma$ -subvariety such that  $\phi$  factors through  $Z$  then  $\phi(X) \subset Z$ .*

*Proof.* Let  $\mathfrak{a}$  denote the kernel of  $\phi^*: k\{Y\} \rightarrow k\{X\}$  and set  $\phi(X) = \mathbb{V}(\mathfrak{a}) \subset Y$ . As  $\phi^*$  factors through  $k\{Y\} \rightarrow k\{\phi(X)\} = k\{Y\}/\mathfrak{a}$ , we see that  $\phi$  factors through  $\phi(X)$ . If  $\phi$  factors through  $Z$ , i.e.,  $\phi^*$  factors through  $k\{Y\} \rightarrow k\{Z\} = k\{Y\}/\mathbb{I}(Z)$ , then clearly  $\mathbb{I}(Z) \subset \mathfrak{a}$ . So  $\phi(X) \subset Z$ .  $\square$

Note that  $\phi(X)$  is the  $\sigma$ -closure of  $\text{Im}(\phi)$  in the sense that

$$\mathbb{I}(\phi(X)) = \{f \in k\{Y\} \mid f(a) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } a \in \text{Im}(\phi)(R)\}.$$

If  $\phi: X \rightarrow Y$  is a morphism of  $\sigma$ -varieties and  $Z \subset X$  is a  $\sigma$ -closed  $\sigma$ -subvariety, then we will write  $\phi(Z)$  for the  $\sigma$ -closed  $\sigma$ -subvariety  $\phi|_Z(Z)$  of  $Y$  where  $\phi|_Z: Z \rightarrow X \xrightarrow{\phi} Y$ .

A morphism  $\phi: X \rightarrow Y$  of  $\sigma$ -varieties is called a  *$\sigma$ -closed embedding* if  $\phi$  induces an isomorphism between  $X$  and a  $\sigma$ -closed  $\sigma$ -subvariety of  $Y$ , i.e.,  $X \rightarrow \phi(X)$  is an isomorphism. We write

$$\phi: X \hookrightarrow Y$$

to express that  $\phi$  is a  $\sigma$ -closed embedding. In analogy to a well known result in algebraic geometry we have:

**Lemma 1.6.** *A morphism  $\phi: X \rightarrow Y$  of  $\sigma$ -varieties is a  $\sigma$ -closed embedding if and only if  $\phi^*: k\{Y\} \rightarrow k\{X\}$  is surjective.*

*Proof.* Let  $\mathfrak{a}$  denote the kernel of  $\phi^*: k\{Y\} \rightarrow k\{X\}$ . The dual map to  $X \rightarrow \phi(X)$  is  $k\{Y\}/\mathfrak{a} \rightarrow k\{X\}$ . It is an isomorphism if and only if  $\phi^*$  is surjective.  $\square$

### 1.3 Base extension

In this subsection we show how to extend the base  $\sigma$ -field of a  $\sigma$ -variety. This is already one of the first points where our more general definition of  $\sigma$ -varieties pays off. For  $\sigma$ -varieties in the classical sense of [Lev08] and [Coh65] base extension is not at all well-behaved. For example, the system of algebraic difference equations

$$y^2 = 2, \sigma(y) = -y$$

clearly has a solution in a  $\sigma$ -field extension of  $\mathbb{Q}$ , where we consider  $\mathbb{Q}$  as a  $\sigma$ -field via the identity map. However, if we consider the system over the  $\sigma$ -field  $\mathbb{C}$ , where again  $\sigma$  is the identity map on  $\mathbb{C}$ , then the system has no solution in a  $\sigma$ -field extension of  $\mathbb{C}$ . See Chapter 8, Section 6 in [Coh65] for more details on base extension for  $\sigma$ -varieties in the classical sense. Since we consider solutions in arbitrary  $k$ - $\sigma$ -algebras and not just in  $\sigma$ -field extensions of  $k$  these problems disappear.

Let  $k$  be a  $\sigma$ -field and  $X$  a  $\sigma$ -variety over  $k$ . Moreover, let  $k'$  be a  $\sigma$ -field extension of  $k$ . We can define a functor

$$X_{k'}$$

from  $k'$ - $\sigma$ -Alg to Sets by  $X_{k'}(R') = X(R')$  for any  $k'$ - $\sigma$ -algebra  $R'$ . Then  $X_{k'}$  is a  $\sigma$ -variety over  $k'$ . Indeed,

$$k'\{X_{k'}\} = k\{X\} \otimes_k k'.$$

In terms of equations, this of course simply means that a system  $F \subset k\{y\} = k\{y_1, \dots, y_n\}$  of algebraic difference equations over  $k$  is considered as a system  $F \subset k'\{y\}$  of algebraic difference equations over  $k'$ . So if  $k\{X\} = k\{y\}/[F]$  then  $k'\{X_{k'}\} = k'\{y\}/[F]$ .

### 1.4 Zariski closures

In this subsection we show how a variety over a  $\sigma$ -field can be considered as a  $\sigma$ -variety. We also introduce the important Zariski closures of a  $\sigma$ -subvariety of a variety. Cf. Sections A.4 and A.5 in [DVHW14].

Let  $k$  be a  $\sigma$ -field and  $\mathcal{X}$  a variety over  $k$ , where, for our purposes, a variety over  $k$  is an affine scheme of finite type over  $k$ . For a  $k$ - $\sigma$ -algebra  $R$  let

$$R^\sharp$$

denote the  $k$ -algebra obtained from  $R$  by forgetting  $\sigma$ . We can define a functor  $[\sigma]_k \mathcal{X}$  from  $k$ - $\sigma$ -Alg to Sets by

$$[\sigma]_k \mathcal{X}(R) = \mathcal{X}(R^\sharp)$$

for any  $k$ - $\sigma$ -algebra  $R$ . Our next goal is to show that  $[\sigma]_k \mathcal{X}$  is  $\sigma$ -variety over  $k$ . That is, we need to construct  $k\{[\sigma]_k \mathcal{X}\}$ . By doing so, we also introduce some notations that will be useful later on.

Let  $A$  be a  $k$ -algebra. For every  $i \geq 0$  let

$$\sigma^i A = A \otimes_k k,$$

where the tensor product is formed by using  $\sigma^i: k \rightarrow k$  on the right hand side. We consider  $\sigma^i A$  as  $k$ -algebra via the right factor. We set

$$A[i] = A \otimes_k \sigma A \otimes_k \cdots \otimes_k \sigma^i A.$$

We have inclusions  $A[i] \hookrightarrow A[i+1]$  of  $k$ -algebras and the limit, i.e, the union

$$[\sigma]_k A$$

of the  $A[i]$ 's is a  $k$ - $\sigma$ -algebra where for  $(r_0 \otimes \lambda_0) \otimes \cdots \otimes (r_i \otimes \lambda_i) \in \sigma^0 A \otimes_k \cdots \otimes_k \sigma^i A = A[i]$  the map  $\sigma: [\sigma]_k A \rightarrow [\sigma]_k A$  is given by

$$\sigma((r_0 \otimes \lambda_0) \otimes \cdots \otimes (r_i \otimes \lambda_i)) = (1 \otimes 1) \otimes (r_0 \otimes \sigma(\lambda_0)) \otimes \cdots \otimes (r_i \otimes \sigma(\lambda_i)) \in A[i+1].$$

The inclusion  $A = A[0] \hookrightarrow [\sigma]_k A$  is characterized by the following universal property.



**Lemma 1.7.** *For every  $k$ -algebra  $A$  there exists a  $k$ - $\sigma$ -algebra  $[\sigma]_k A$  and a morphism  $\psi: A \rightarrow [\sigma]_k A$  of  $k$ -algebras such that for every  $k$ - $\sigma$ -algebra  $R$  and every morphism  $\psi': A \rightarrow R$  of  $k$ -algebras there exists a unique morphism  $\varphi: [\sigma]_k A \rightarrow R$  of  $k$ - $\sigma$ -algebras making*

$$\begin{array}{ccc} A & \xrightarrow{\psi} & [\sigma]_k A \\ & \searrow \psi' & \swarrow \varphi \\ & R & \end{array}$$

commutative. □

In other words,

$$\mathrm{Hom}([\sigma]_k A, R) \simeq \mathrm{Hom}(A, R^\#) \quad (3)$$

and  $[\sigma]_k$  is left adjoint to the forgetful functor  $(-)^{\#}$ .

**Example 1.8.** If  $A = k[y_1, \dots, y_n]$ , then  $[\sigma]_k A = k\{y_1, \dots, y_n\}$ . More generally, if  $A = k[y_1, \dots, y_n]/(F)$ , then  $[\sigma]_k A = k\{y_1, \dots, y_n\}/[F]$ .

Let  $k[\mathcal{X}]$  denote the coordinate ring of the variety  $\mathcal{X} = \mathrm{Hom}(k[\mathcal{X}], -)$ . Then (3) with  $A = k[\mathcal{X}]$  shows that  $[\sigma]_k \mathcal{X}$  is represented by  $[\sigma]_k k[\mathcal{X}]$ . If  $M \subset k[\mathcal{X}]$  generates  $k[\mathcal{X}]$  as a  $k$ -algebra, then  $M \subset [\sigma]_k k[\mathcal{X}]$  generates  $[\sigma]_k k[\mathcal{X}]$  as a  $k$ - $\sigma$ -algebra. Therefore  $[\sigma]_k \mathcal{X}$  is a  $\sigma$ -variety over  $k$ . Indeed,  $k\{[\sigma]_k \mathcal{X}\} = [\sigma]_k k[\mathcal{X}]$ . In the sequel, if confusion is unlikely we will often write  $\mathcal{X}$  instead of  $[\sigma]_k \mathcal{X}$ . In particular, we will write  $k\{\mathcal{X}\}$  instead of  $k\{[\sigma]_k \mathcal{X}\}$  and by a  $\sigma$ -closed  $\sigma$ -subvariety of a variety  $\mathcal{X}$ , we mean a  $\sigma$ -closed  $\sigma$ -subvariety of  $[\sigma]_k \mathcal{X}$ .

Of course  $[\sigma]_k$  is a functor from the category of varieties over  $k$  to the category of  $\sigma$ -varieties over  $k$ : If  $\phi: \mathcal{X} \rightarrow \mathcal{Y}$  is a morphism of varieties, then we can define  $[\sigma]_k(\phi): [\sigma]_k \mathcal{X} \rightarrow [\sigma]_k \mathcal{Y}$  by

$$([\sigma]_k(\phi))_R: ([\sigma]_k \mathcal{X})(R) = \mathcal{X}(R^\#) \xrightarrow{\phi_{R^\#}} \mathcal{Y}(R^\#) = ([\sigma]_k \mathcal{Y})(R)$$

for any  $k$ - $\sigma$ -algebra  $R$ .

Next we will introduce the Zariski closures of a  $\sigma$ -closed  $\sigma$ -subvariety of a variety. We will use notations for varieties similar to the ones introduced for  $k$ -algebras above: If  $\mathcal{X}$  is a variety over  $k$  and  $i \geq 1$ , then

$$\sigma^i \mathcal{X}$$

denotes the variety over  $k$  obtained from  $\mathcal{X}$  by base extension via  $\sigma^i: k \rightarrow k$ . Similarly, if  $\phi: \mathcal{X} \rightarrow \mathcal{Y}$  is a morphism of varieties over  $k$ , then  $\sigma^i \phi: \sigma^i \mathcal{X} \rightarrow \sigma^i \mathcal{Y}$  denotes the morphism of varieties over  $k$  obtained from  $\phi$  by base extension via  $\sigma^i: k \rightarrow k$ . We also set

$$\mathcal{X}[i] = \mathcal{X} \times^\sigma \mathcal{X} \times \cdots \times \sigma^i \mathcal{X}.$$

Let  $Y$  be a  $\sigma$ -closed  $\sigma$ -subvariety of  $\mathcal{X}$ . Then  $Y$  is defined by a  $\sigma$ -ideal  $\mathbb{I}(Y) \subset k\{\mathcal{X}\} = \cup_{i \geq 0} k[\mathcal{X}[i]]$ . For  $i \geq 0$ , the closed subvariety

$$Y[i]$$

of  $\mathcal{X}[i]$  defined by  $\mathbb{I}(Y) \cap k[\mathcal{X}[i]] \subset k[\mathcal{X}[i]]$  is called the  $i$ -th order Zariski closure of  $Y$  in  $\mathcal{X}$ . The 0-th order Zariski closure of  $Y$  in  $\mathcal{X}$  is also the Zariski closure of  $Y$  in  $\mathcal{X}$ . We say that  $Y$  is Zariski dense in  $\mathcal{X}$  if the Zariski closure of  $Y$  in  $\mathcal{X}$  equals  $\mathcal{X}$ . Note that  $Y$  is Zariski dense in  $\mathcal{X}$  if and only if  $k[\mathcal{X}] \rightarrow k\{Y\}$  is injective.

For  $i \geq 1$  we have morphisms of varieties

$$\pi_i: \mathcal{X}[i] \rightarrow \mathcal{X}[i-1], (x_0, \dots, x_i) \mapsto (x_0, \dots, x_{i-1})$$

and

$$\sigma_i: \mathcal{X}[i] \rightarrow \sigma(\mathcal{X}[i-1]) = \sigma \mathcal{X} \times \cdots \times \sigma^i \mathcal{X}, (x_0, \dots, x_i) \mapsto (x_1, \dots, x_i)$$

that form a commutative diagram:

$$\begin{array}{ccc} \mathcal{X}[i] & \xrightarrow{\pi_i} & \mathcal{X}[i-1] \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ \sigma(\mathcal{X}[i-1]) & \xrightarrow{\sigma \pi_{i-1}} & \sigma(\mathcal{X}[i-2]) \end{array}$$

There are induced morphisms  $\pi_i: Y[i] \rightarrow Y[i-1]$  of varieties over  $k$ , and since  $\mathbb{I}(Y) \subset k\{\mathcal{X}\}$  is a  $\sigma$ -ideal, we also have induced morphisms  $\sigma_i: Y[i] \rightarrow {}^\sigma(Y[i-1])$  of varieties over  $k$ .

## 2 Basic definitions

In this section we introduce  $\sigma$ -algebraic groups and give some examples. We also show that every  $\sigma$ -algebraic group is isomorphic to a  $\sigma$ -closed subgroup of the general linear group.

From now on we will work over a fixed  $\sigma$ -field  $k$ . By an algebraic group over  $k$ , we mean an affine group scheme of finite type over  $k$ . (So an algebraic group need not be smooth.) Since the category of  $\sigma$ -varieties has products and a terminal object (Remark 1.3) the following definition makes sense.

**Definition 2.1.** *Let  $k$  be a  $\sigma$ -field. A  $\sigma$ -algebraic group over  $k$  is a group object in the category of  $\sigma$ -varieties over  $k$ .*

Alternatively, we could define a  $\sigma$ -algebraic group as functor from  $k\text{-}\sigma\text{-Alg}$  to **Groups**, the category of groups, which is representable by a finitely  $\sigma$ -generated  $k\text{-}\sigma$ -algebra. A *morphism of  $\sigma$ -algebraic groups* is of course a morphism of  $\sigma$ -varieties that respects the group structure. A  *$\sigma$ -closed embedding* of  $\sigma$ -algebraic groups is a morphism of  $\sigma$ -algebraic groups which is a  $\sigma$ -closed embedding of  $\sigma$ -varieties.

**Definition 2.2.** *Let  $k$  be a  $\sigma$ -field. A  $k\text{-}\sigma$ -Hopf algebra is a Hopf algebra  $A$  over  $k$  with the structure of a  $k\text{-}\sigma$ -algebra such that the Hopf-algebra structure maps  $\Delta: A \rightarrow A \otimes_k A$ ,  $S: A \rightarrow A$  and  $\varepsilon: A \rightarrow k$  are morphisms of  $k\text{-}\sigma$ -algebras.*

A  *$k\text{-}\sigma$ -Hopf subalgebra* of a  $k\text{-}\sigma$ -Hopf algebra is a Hopf subalgebra which is a  $k\text{-}\sigma$ -subalgebra.

**Proposition 2.3.** *The category of  $\sigma$ -algebraic groups over  $k$  is anti-equivalent to the category of  $k\text{-}\sigma$ -Hopf algebras that are finitely  $\sigma$ -generated over  $k$ .*

*Proof.* This follows from Remark 1.2 in an analogous fashion to Theorem 1.4 in [Wat79].  $\square$

Let  $G$  be a  $\sigma$ -algebraic group. A  *$\sigma$ -closed subgroup  $H$  of  $G$*  is a  $\sigma$ -closed  $\sigma$ -subvariety  $H$  of  $G$  such that  $H(R)$  is a subgroup of  $G(R)$  for any  $k\text{-}\sigma$ -algebra  $R$ . Then  $H$  itself is a  $\sigma$ -algebraic group. We write

$$H \leq G$$

to express that  $H$  is a  $\sigma$ -closed subgroup of  $G$ . If  $H_1$  and  $H_2$  are  $\sigma$ -closed subgroups of  $G$ , then  $H_1 \cap H_2$  is also a  $\sigma$ -closed subgroup of  $G$ .

Let  $A$  be  $k\text{-}\sigma$ -Hopf algebra. A Hopf ideal of  $A$  is called a  *$\sigma$ -Hopf ideal* if it is a  $\sigma$ -ideal. In analogy to Section 2.1 in [Wat79] it follows from Lemma 1.4 that:

**Lemma 2.4.** *Let  $G$  be a  $\sigma$ -algebraic  $G$ . There is a one-to-one correspondence between the  $\sigma$ -closed subgroups of  $G$  and the  $\sigma$ -Hopf ideals in  $k\{G\}$ .*  $\square$

**Example 2.5.** Let  $V$  be a finite dimensional  $k$ -vector space. For every  $k\text{-}\sigma$ -algebra  $R$  let  $\text{GL}(V)(R)$  denote the group of  $R$ -linear automorphisms of  $V \otimes_k R$ . Then  $\text{GL}(V)$  is naturally a functor from  $k\text{-}\sigma\text{-Alg}$  to **Groups**. Indeed,  $\text{GL}(V)$  is a  $\sigma$ -algebraic group: By choosing a basis  $v_1, \dots, v_n$  of  $V$ , we can identify  $\text{GL}(V)(R)$  with  $\text{GL}_n(R)$  and  $\text{GL}(V)$  is represented by

$$k\{\text{GL}_n\} = k\{x_{ij}, \frac{1}{\det(x)}\}.$$

More generally:

**Example 2.6.** Every algebraic group over  $k$  can be interpreted as a  $\sigma$ -algebraic group over  $k$ . Here, as throughout the text, by an algebraic group over  $k$  we mean an affine group scheme of finite type over  $k$ . Indeed, let  $\mathcal{G}$  be an algebraic group over  $k$  and as in Section 1.4, let  $R^\sharp$  denote the  $k$ -algebra obtained from the  $k\text{-}\sigma$ -algebra  $R$  by forgetting  $\sigma$ . Then

$$R \rightsquigarrow \mathcal{G}(R^\sharp)$$

is a functor from  $k\text{-}\sigma\text{-Alg}$  to **Groups**, i.e.,  $[\sigma]_k \mathcal{G}$  is a  $\sigma$ -algebraic group.

We will often write  $\mathcal{G}$  instead of  $[\sigma]_k \mathcal{G}$ . In particular, by a  $\sigma$ -closed subgroup of  $\mathcal{G}$  we mean a  $\sigma$ -closed subgroup of  $[\sigma]_k \mathcal{G}$ .

**Example 2.7.** Let  $0 \leq \alpha_1 < \dots < \alpha_n$  and  $1 \leq \beta_1, \dots, \beta_n$  be integers. We can define a  $\sigma$ -closed subgroup  $G$  of the multiplicative group  $\mathbb{G}_m$  by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\} \leq \mathbb{G}_m(R)$$

for every  $k$ - $\sigma$ -algebra  $R$ .

**Example 2.8.** Every homogeneous linear difference equation  $\sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \dots + \lambda_0 y = 0$  over  $k$  defines a  $\sigma$ -closed subgroup  $G$  of the additive group  $\mathbb{G}_a$ , i.e.,

$$G(R) = \{g \in R \mid \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \dots + \lambda_0 g = 0\} \leq \mathbb{G}_a(R)$$

for any  $k$ - $\sigma$ -algebra  $R$ .

**Example 2.9.** The equations of the unitary group define a  $\sigma$ -closed subgroup of the general linear group:

$$G(R) = \{g \in \mathrm{GL}_n(R) \mid g\sigma(g)^T = \sigma(g)^T g = I_n\} \leq \mathrm{GL}_n(R)$$

for any  $k$ - $\sigma$ -algebra  $R$ .

Example 2.9 can be generalized as follows:

**Example 2.10.** Let  $k$  be a  $\sigma$ -field,  $n \geq 1$  an integer,  $\mathcal{G}$  an algebraic group over  $k$  and  $\phi: \mathcal{G} \rightarrow \sigma^n \mathcal{G}$  a morphism of algebraic groups over  $k$ . There is a morphism  $\sigma^n: \mathcal{G} \rightarrow \sigma^n \mathcal{G}$  of  $\sigma$ -algebraic groups over  $k$ , which, in terms of equations is given by applying  $\sigma^n$  to the coordinates. In terms of  $k$ - $\sigma$ -algebras this morphism can be described as  $\sigma^n(k\{\mathcal{G}\}) = k\{\mathcal{G}\} \otimes_k k \rightarrow k\{\mathcal{G}\} \otimes_k k \rightarrow k\{\mathcal{G}\}$   $f \otimes \lambda \mapsto \sigma^n(f)\lambda$ . We can define a  $\sigma$ -closed subgroup  $G$  of  $\mathcal{G}$  by

$$G(R) = \{g \in \mathcal{G}(R) \mid \sigma^n(g) = \psi(g)\} \leq \mathcal{G}(R)$$

for any  $k$ - $\sigma$ -algebra  $R$ .

**Example 2.11.** Let  $k$  be a field of positive characteristic  $p$  and  $q$  be a power of  $p$ . Consider  $k$  as a  $\sigma$ -field via the Frobenius, i.e.,  $\sigma(\lambda) = \lambda^q$  for  $\lambda \in k$ . An algebraic group  $\mathcal{G}$  over  $k$  can be considered as a  $\sigma$ -algebraic group over  $k$ : We turn  $k[\mathcal{G}]$  into a  $k$ - $\sigma$ -algebra by setting  $\sigma(f) = f^q$  for  $f \in k[\mathcal{G}]$ . Then clearly  $k[\mathcal{G}]$  is a  $k$ - $\sigma$ -Hopf algebra.

A  $\sigma$ -algebraic group as in Example 2.11 will be called a *Frobenius algebraic group*.

**Example 2.12.** Let  $k$  be a  $\sigma$ -field,  $\mathbf{G}$  a finite group and  $\Sigma: \mathbf{G} \rightarrow \mathbf{G}$  a group endomorphism. Let  $A$  be the  $k$ -vector space with basis  $(e_g)_{g \in \mathbf{G}}$ . We consider it as  $k$ -algebra via

$$(\sum \lambda_g e_g)(\sum \mu_g e_g) = \sum \lambda_g \mu_g e_g.$$

We can define a Hopf algebra structure on  $A$  by

$$\Delta(e_g) = \sum_{(g_1, g_2)} e_{g_1} \otimes e_{g_2},$$

where the sum ranges over all pairs  $(g_1, g_2) \in \mathbf{G}^2$  such that  $g_1 g_2 = g$ ,  $S(e_g) = e_{g^{-1}}$  and  $\varepsilon(e_g) = 0$  for  $g \neq 1$  and  $\varepsilon(e_1) = 1$ . The algebraic group corresponding to  $A$  is usually called the constant group scheme for  $\mathbf{G}$ . (See [Wat79, Section 2.3].) Extend  $\sigma: k \rightarrow k$  to  $\sigma: A \rightarrow A$  by  $\sigma(e_g) = \sum_h e_h$ , where the sum is taken over all  $h \in \mathbf{G}$  such that  $\Sigma(h) = g$ . This defines a  $k$ - $\sigma$ -algebra structure on  $A$  and therefore we obtain an associated  $\sigma$ -algebraic group  $G = \mathrm{Hom}(A, -)$ .

Similar to algebraic groups,  $\sigma$ -algebraic groups can be linearized:

**Theorem 2.13.** *Let  $G$  be a  $\sigma$ -algebraic group over  $k$ . Then there exists a finite dimensional  $k$ -vector space  $V$  and a  $\sigma$ -closed embedding  $G \hookrightarrow \mathrm{GL}(V)$ . In particular,  $G$  is isomorphic to a  $\sigma$ -closed subgroup of  $\mathrm{GL}_n$  for some  $n \geq 1$ .*

*Proof.* Assume that  $f_1, \dots, f_m \in k\{G\}$  generate  $k\{G\}$  as a  $k$ - $\sigma$ -algebra. By [Wat79, Section 3.3, p. 24] there exists a Hopf subalgebra  $A$  of  $k\{G\}$  which contains  $f_1, \dots, f_m$  and is finitely generated as a  $k$ -algebra. By [Wat79, Section 3.4, p. 25] there exists an integer  $n \geq 1$  and a surjective morphism  $k[\mathrm{GL}_n] \rightarrow A$  of Hopf algebras. By Lemma 1.7 the morphism  $k[\mathrm{GL}_n] \rightarrow A \hookrightarrow k\{G\}$  of  $k$ -algebras extends to a morphism  $k\{\mathrm{GL}_n\} \rightarrow k\{G\}$  of  $k$ - $\sigma$ -algebras. Indeed, this is a morphism of  $k$ - $\sigma$ -Hopf algebras and since  $f_1, \dots, f_m$  lie in the image, it is surjective. Now the claim follows from Lemma 1.6.  $\square$

### 3 Zariski closures of difference algebraic groups and the growth group

In this section we show that the eventual growth of the Zariski closures of a  $\sigma$ -closed subgroup  $G$  of an algebraic group  $\mathcal{G}$  is governed by an algebraic group, called the growth group of  $G$  (with respect to the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ ). We also introduce the  $\sigma$ -dimension and the order of a  $\sigma$ -algebraic group  $G$ .

Let  $k$  be a  $\sigma$ -field and  $\mathcal{G}$  an algebraic group over  $k$ . Then, for ever  $i \geq 0$ ,  $\sigma^i \mathcal{G}$  and  $\mathcal{G}[i] = \mathcal{G} \times^\sigma \mathcal{G} \times \cdots \times^\sigma \mathcal{G}$  (see Section 1.4) are naturally algebraic groups over  $k$ . For every  $i \geq 1$  the maps  $\pi_i: \mathcal{G}[i] \rightarrow \mathcal{G}[i-1]$  and  $\sigma_i: \mathcal{G}[i] \rightarrow \sigma(\mathcal{G}[i-1])$  are morphisms of algebraic groups over  $k$ .

Let  $G$  be a  $\sigma$ -closed subgroup of  $\mathcal{G}$ . For every  $i \geq 0$  we have an inclusion  $k[\mathcal{G}[i]] \subset k\{\mathcal{G}\}$  of Hopf algebras. Since  $\mathbb{I}(G) \subset k\{\mathcal{G}\}$  is a Hopf ideal,  $\mathbb{I}(G) \cap k[\mathcal{G}[i]]$  is a Hopf ideal of  $k[\mathcal{G}[i]]$ . So the  $i$ -th order Zariski closure  $G[i]$  of  $G$  in  $\mathcal{G}$  is a closed subgroup of  $\mathcal{G}[i]$ . The maps  $\pi_i: G[i] \rightarrow G[i-1]$  and  $\sigma_i: G[i] \rightarrow \sigma(G[i-1])$  are morphisms of algebraic groups over  $k$  and form a commutative diagram:

$$\begin{array}{ccc} G[i] & \xrightarrow{\pi_i} & G[i-1] \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ \sigma(G[i-1]) & \xrightarrow{\sigma\pi_{i-1}} & \sigma(G[i-2]) \end{array} \quad (4)$$

For  $i \geq 1$  we set

$$\mathcal{G}_i = \ker(\pi_i) \leq G[i].$$

We also set  $\mathcal{G}_0 = G[0]$ . Because of (4) we have induced morphisms  $\sigma_i: \mathcal{G}_i \rightarrow \sigma(\mathcal{G}_{i-1})$  of algebraic groups over  $k$ .

**Proposition 3.1.** *For every  $i \geq 1$  the map  $\sigma_i: \mathcal{G}_i \rightarrow \sigma(\mathcal{G}_{i-1})$  is a closed embedding and there exists an integer  $m \geq 1$  such that  $\sigma_i: \mathcal{G}_i \rightarrow \sigma(\mathcal{G}_{i-1})$  is an isomorphism for every  $i \geq m$ .*

*Proof.* Let us start by describing  $\sigma_i$  in algebraic terms. Assume that  $a = (a_1, \dots, a_n)$  generates  $k[\mathcal{G}]$  as a  $k$ -algebra and let  $\bar{a}$  denote the image of  $a$  in  $k\{G\}$ . So

$$k[\mathcal{G}] = k[a] \subset k[a, \sigma(a), \dots] = k\{\mathcal{G}\}$$

and  $k[G[i]] = k[\bar{a}, \dots, \sigma^i(\bar{a})]$ . The morphism  $\sigma_i: G[i] \rightarrow \sigma(G[i-1])$  corresponds to the map

$$\sigma(k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]) \longrightarrow k[\bar{a}, \dots, \sigma^i(\bar{a})], \quad f \otimes \lambda \mapsto \sigma(f)\lambda$$

and the morphism  $\sigma_i: \mathcal{G}_i \rightarrow \sigma(\mathcal{G}_{i-1})$  corresponds to the map

$$\begin{aligned} \sigma(k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]) \otimes_{k[\bar{a}, \dots, \sigma^{i-2}(\bar{a})]} k &\longrightarrow k[\bar{a}, \dots, \sigma^i(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]} k \\ (f \otimes \lambda) \otimes \mu &\longmapsto \sigma(f) \otimes \sigma(\lambda)\mu \end{aligned}$$

where the tensor products are formed in virtue of the counit  $\varepsilon: k\{G\} \rightarrow k$ . Since  $k[\bar{a}, \dots, \sigma^i(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]} k$  is generated as a  $k$ -algebra by the image of  $\sigma^i(\bar{a})$ , the above map is clearly surjective. Thus  $\sigma_i: \mathcal{G}_i \rightarrow \sigma(\mathcal{G}_{i-1})$  is a closed embedding.

To prove the second claim of the proposition, let us first assume that  $k$  is inversive. The map

$$\begin{aligned} \psi_i: k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-2}(\bar{a})]} k &\longrightarrow k[\bar{a}, \dots, \sigma^i(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]} k \\ f \otimes \lambda &\longmapsto \sigma(f) \otimes \sigma(\lambda) \end{aligned}$$

does not respect the  $k$ -algebra structure, but since  $k$  is inversive, it is surjective. We thus have a descending chain of closed subschemes

$$\mathcal{G}_0 \hookleftarrow \mathcal{G}_1 \hookleftarrow \mathcal{G}_2 \cdots$$

Since  $\mathcal{G}_0$  is of finite type over  $k$ , this sequence must stabilize. That is, there exists an integer  $m \geq 1$  such that  $\psi_i$  is bijective for every  $i \geq m$ . Since  $k$  is inversive,  $k[\mathcal{G}_i] \rightarrow \sigma(k[\mathcal{G}_i])$ ,  $f \mapsto f \otimes 1$  is bijective. It follows that for  $i \geq m$ , the morphism  $\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_i]$  dual to  $\sigma_i$  is an isomorphism, since it can be obtained as the composition  $\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_{i-1}] \xrightarrow{\psi} k[\mathcal{G}_i]$  of two bijective maps. This proves the proposition for  $k$  inversive.

The general case can be reduced to the inversive case: Let  $k^*$  denote the inversive closure of  $k$  ([Lev08, Definition 2.1.6]). So, in particular,  $k^*$  is an inversive  $\sigma$ -field extension of  $k$ . The formation of Zariski-closures and of the  $\mathcal{G}_i$  is compatible with base extension. It therefore follows from the inversive case, that there exists an integer  $m \geq 1$  such that for every  $i \geq m$  the morphism  $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$  becomes an isomorphism after base extension from  $k$  to  $k^*$ . But then already  $\sigma_i$  must be an isomorphism for  $i \geq m$ .  $\square$

Proposition 3.1 allows us to associate to the inclusion  $G \leq \mathcal{G}$  an algebraic group, which measures the (eventual) growth of the Zariski closures  $G[i]$  of  $G$  in  $\mathcal{G}$ .

**Definition 3.2.** Let  $\mathcal{G}$  be an algebraic group and  $G \leq \mathcal{G}$  a  $\sigma$ -closed subgroup. For  $i \geq 1$  let  $\mathcal{G}_i$  denote the kernel of the projection  $\pi_i: G[i] \rightarrow G[i-1]$  between the Zariski closures of  $G$  in  $\mathcal{G}$ . Let  $m \geq 0$  denote the smallest integer such that  $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$  is an isomorphism for every  $i > m$ . Then  $\mathcal{G}_m$  is called the growth group of  $G$  with respect to the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ .

**Example 3.3.** Let  $0 \leq \alpha_1 < \dots < \alpha_n$  and  $1 \leq \beta_1, \dots, \beta_n$  be integers and  $G \leq \mathbb{G}_m$  the  $\sigma$ -closed subgroup of the multiplicative group  $\mathbb{G}_m$  given by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\}$$

for every  $k$ - $\sigma$ -algebra  $R$ . Then the growth group of  $G$  with respect to the given embedding  $G \hookrightarrow \mathbb{G}_m$  is  $\mu_{\beta_n}$ , where  $\mu_{\beta_n}(R) = \{g \in R^\times \mid g^{\beta_n} = 1\}$  for every  $k$ -algebra  $R$ .

The following example shows that the growth group does indeed depend on the embedding  $G \hookrightarrow \mathcal{G}$  and therefore is not an invariant of  $G$ .

**Example 3.4.** Let  $G = \mathbb{G}_m$  (considered as a  $\sigma$ -algebraic group). For  $n \geq 1$  the  $\sigma$ -closed embedding

$$G \rightarrow \mathbb{G}_m^2, g \mapsto (g, \sigma(g)^n)$$

identifies  $G$  with the  $\sigma$ -closed subgroup  $G \leq \mathbb{G}_m^2$  given by

$$G(R) = \{(g_1, g_2) \in \mathbb{G}_m(R)^2 \mid \sigma(g_1)^n = g_2\}$$

for any  $k$ - $\sigma$ -algebra  $R$ . The growth group of  $G$  with respect to the embedding  $G \hookrightarrow \mathbb{G}_m^2$  is  $\mu_n \times \mathbb{G}_m$ .

Even though the growth group itself does depend on the chosen embedding  $G \hookrightarrow \mathcal{G}$ , it carries some information which only depends on  $G$ . We will now show that the dimension of the growth group does not depend on the embedding  $G \hookrightarrow \mathcal{G}$ . In Section 6 we will see that also the size of the growth group is independent of the chosen embedding.

The following theorem can be seen as a group theoretic analog of the classical theorem on the existence of the so-called dimension polynomial of an extension of  $\sigma$ -fields ([Lev08, Theorem 4.2.1]). See also [Hru04, Lemma 4.21].

**Theorem 3.5.** Let  $\mathcal{G}$  be an algebraic group and  $G \leq \mathcal{G}$  a  $\sigma$ -closed subgroup. For  $i \geq 0$  let  $d_i = \dim(G[i])$  denote the dimension of the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}$ . Then there exist integers  $d, e \geq 0$  such that

$$d_i = d(i+1) + e \text{ for } i \gg 0.$$

The integer  $d$  only depends on  $G$  and not on the choice of  $\mathcal{G}$  and the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ . If  $d = 0$ , the integer  $e$  only depends on  $G$  and not on the choice of  $\mathcal{G}$  and the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ .

*Proof.* Let  $\mathcal{G}_i$  denote the kernel of  $G[i] \rightarrow G[i-1]$ . Then  $\dim(G[i]) = \dim(G[i-1]) + \dim(\mathcal{G}_i)$ . Let  $m \geq 0$  denote the smallest integer such that  $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$  is an isomorphism for every  $i > m$ . It follows that for  $i \gg 0$

$$\begin{aligned} \dim(G[i]) &= \dim(\mathcal{G}_i) + \dots + \dim(\mathcal{G}_0) = \\ &= (i - m + 1) \dim(\mathcal{G}_m) + \dim(\mathcal{G}_{m-1}) + \dots + \dim(\mathcal{G}_0) = \\ &= (i + 1) \dim(\mathcal{G}_m) + \dim(\mathcal{G}_{m-1}) + \dots + \dim(\mathcal{G}_0) - m \dim(\mathcal{G}_m) = \\ &= d(i + 1) + e. \end{aligned}$$

It follows from Proposition 3.1 that  $e \geq 0$ .

Let us now show that  $d$  is independent of the chosen embedding  $G \hookrightarrow \mathcal{G}$ . So let  $G \hookrightarrow \mathcal{G}'$  be another  $\sigma$ -closed embedding. Let  $G[i']$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}'$  and let  $d'_i, d', e'$  have the analogous meaning. We have to show that  $d = d'$ .

Let  $a$  be a finite tuple from  $k\{G\}$  which generates  $k[G[0]] \subset k\{G\}$  as a  $k$ -algebra. Similarly, let  $a'$  be a finite tuple from  $k\{G\}$  which generates  $k[G[0]'] \subset k\{G\}$  as a  $k$ -algebra. Then  $k[G[i]] = k[a, \dots, \sigma^i(a)]$  and there exists an integer  $n \geq 0$  such that all coordinates of  $a'$  lie in  $k[G[n]]$ . Then

$$k[G[i']] = k[a', \dots, \sigma^i(a')] \subset k[a, \dots, \sigma^{n+i}(a)] = k[G[n+i]].$$

Therefore  $d'_i \leq d_{n+i}$  and for  $i \gg 0$  we have  $d'(i+1) + e' \leq d(n+i+1) + e$ . Letting  $i$  tend to infinity we find  $d' \leq d$ . By symmetry,  $d' = d$ .

Let us now assume that  $d = 0$ . We have to show that  $e$  does not depend on the choice of the embedding  $G \hookrightarrow \mathcal{G}$ . Do to this we will show that

$$e = \max \{ \dim(R) \mid R \text{ is a finitely generated } k\text{-subalgebra of } k\{G\} \}. \quad (5)$$

For  $i \gg 0$  the finitely generated  $k$ -subalgebra  $k[G[i]]$  of  $k\{G\}$  has dimension  $e$ . Conversely, if  $R$  is a finitely generated  $k$ -subalgebra of  $k\{G\}$ , then  $R$  is contained in some  $k[G[i]]$  and therefore  $\dim(R) \leq e$ . This proves (5).  $\square$

**Definition 3.6.** Let  $G$  be a  $\sigma$ -algebraic group. The integer  $d \geq 0$  defined in Theorem 3.5 above is called the  $\sigma$ -dimension of  $G$  and denoted by

$$\sigma\text{-dim}(G).$$

If  $\sigma\text{-dim}(G) = 0$ , the integer  $e \geq 0$  defined in Theorem 3.5 is called the order of  $G$  and denoted by

$$\text{ord}(G).$$

If  $G$  has positive  $\sigma$ -dimension the order of  $G$  is defined to be infinity.

**Example 3.7.** Let  $\mathcal{G}$  be an algebraic group. Then  $\sigma\text{-dim}([\sigma]_k \mathcal{G}) = \dim(\mathcal{G})$ . Indeed, if we tautologically consider  $G = [\sigma]_k \mathcal{G}$  as a  $\sigma$ -closed subgroup of  $\mathcal{G}$ , then  $G[i] = \mathcal{G} \times {}^\sigma \mathcal{G} \times \dots \times {}^{\sigma^i} \mathcal{G}$  and so  $\dim(G[i]) = \dim(\mathcal{G})(i+1)$  for every  $i \geq 0$ . This also shows that either  $\text{ord}(G) = \infty$  (if  $\dim(\mathcal{G}) > 0$ ) or  $\text{ord}(G) = 0$  if  $(\dim(\mathcal{G}) = 0)$ .

The following example does motivate the naming ‘‘order’’.

**Example 3.8.** Let  $f = \sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \dots + \lambda_0 y$  be a linear difference equation and  $G$  the  $\sigma$ -closed subgroup of  $\mathbb{G}_a$  defined by  $f$ . Then  $\text{ord}(G) = n$ , i.e., the order of  $G$  equals the order of  $f$ .

A certain numerical invariant analogous to the order and called the total dimension has been introduced in [Hru04] in a different setting. We have chosen to stick to the more traditional naming from [Lev08] and [Coh65], also for the sake of the beauty of the formulation of Theorem 13.1. From the proof of Theorem 3.5, we immediately obtain:

**Corollary 3.9.** Let  $G$  be a  $\sigma$ -algebraic group. Then the dimension of the growth group of  $G$  with respect to some  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$  of  $G$  into some algebraic group  $\mathcal{G}$  equals the  $\sigma$ -dimension of  $G$ . In particular, the dimension of the growth group does not depend on the choice of the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ .  $\square$

To state the next proposition we need some more definitions. A  $\sigma$ -ring  $R$  is called a  $\sigma$ -domain if  $R$  is an integral domain and  $\sigma: R \rightarrow R$  is injective. If  $R$  is a  $\sigma$ -domain, the field of fractions of  $R$  is naturally a  $\sigma$ -field.

A  $\sigma$ -algebraic group  $G$  is called *integral* if  $k\{G\}$  is an integral domain. A  $\sigma$ -algebraic group  $G$  is called  $\sigma$ -integral if  $k\{G\}$  is a  $\sigma$ -domain. The  $\sigma$ -transcendence degree of a  $\sigma$ -field extension  $K|k$  is the largest integer  $n \geq 1$  such that the  $\sigma$ -polynomial ring  $k\{y_1, \dots, y_n\}$  may be embedded into  $K$ . (If no such integer exists the  $\sigma$ -transcendence degree is infinite.) See Section 4.1 in [Lev08] for more details on the  $\sigma$ -transcendence degree. The following proposition shows that our notions of dimension and order generalize the classical notions. (See page 394 in [Lev08].)

**Proposition 3.10.** *If  $G$  is a  $\sigma$ -integral  $\sigma$ -algebraic group, then the  $\sigma$ -dimension of  $G$  equals the  $\sigma$ -transcendence degree of the field of fractions of  $k\{G\}$  over  $k$ .*

*If  $G$  is an integral  $\sigma$ -algebraic group, then the order of  $G$  equals the transcendence degree of the field of fractions of  $k\{G\}$  over  $k$ .*

*Proof.* Let us first assume that  $G$  is  $\sigma$ -integral and let us fix a  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ . Assume that  $a = (a_1, \dots, a_n)$  generates  $k[G[0]] \subset k\{G\}$  as a  $k$ -algebra. Let  $K$  denote the field of fractions of  $k\{G\}$ . Since  $G$  is  $\sigma$ -integral  $K$  is naturally a  $\sigma$ -field extension of  $k$  and  $a$  generates  $K$  as a  $\sigma$ -field extension of  $k$ . Since  $\text{trdeg}(k(a, \dots, \sigma^i(a))|k) = \dim(G[i])$ , we see that  $d(t+1) + e$  (with  $d$  and  $e$  as in Theorem 3.5) is really just the difference dimension polynomial (Definition 4.2.2 in [Lev08]) of the  $\sigma$ -field extension  $K|k$  associated with  $a$ . It follows from Theorem 4.2.1 (iii) in [Lev08] that  $\sigma\text{-dim}(G) = d = \sigma\text{-trdeg}(K|k)$ .

Now assume that  $G$  is integral. Let  $K$  denote the field of fractions of  $k\{G\}$ . If  $\sigma\text{-dim}(G) > 0$ , then it is clear from Theorem 3.5 that the transcendence degree of  $K$  over  $k$  is infinite. So  $\text{ord}(G) = \text{trdeg}(K|k)$  in this case.

If  $\sigma\text{-dim}(G) = 0$ , the claim follows from equation (5) above.  $\square$

The  $\sigma$ -dimension is invariant under extension of the base  $\sigma$ -field.

**Lemma 3.11.** *Let  $G$  be a  $\sigma$ -algebraic group and  $k'$  a  $\sigma$ -field extension of  $k$ . Then  $\sigma\text{-dim}(G_{k'}) = \sigma\text{-dim}(G)$  and  $\text{ord}(G_{k'}) = \text{ord}(G)$ .*

*Proof.* Let  $\mathcal{G}$  be an algebraic group such that  $G$  is a  $\sigma$ -closed subgroup of  $\mathcal{G}$ . Then  $G_{k'}$  is a  $\sigma$ -closed subgroup of  $\mathcal{G}_{k'}$  and for  $i \geq 0$  the  $i$ -th order Zariski closure  $G_{k'}[i]$  of  $G_{k'}$  in  $\mathcal{G}_{k'}$  is obtained from the  $i$ -th order Zariski closure  $G[i]$  of  $G$  in  $\mathcal{G}$  by base extension, i.e.,  $G_{k'}[i] = G[i]_{k'}$ . Now the claim of the lemma follows from the fact that the usual dimension is invariant under base extension.  $\square$

For later use we record:

**Lemma 3.12.** *Let  $G$  and  $H$  be  $\sigma$ -algebraic groups. Then  $G \times H$  is a  $\sigma$ -algebraic group with*

$$\sigma\text{-dim}(G \times H) = \sigma\text{-dim}(G) + \sigma\text{-dim}(H)$$

and

$$\text{ord}(G \times H) = \text{ord}(G) + \text{ord}(H).$$

*Proof.* Let  $\mathcal{G}$  and  $\mathcal{H}$  be algebraic groups containing  $G$  and  $H$  as  $\sigma$ -closed subgroups respectively. Then  $G \times H$  is a  $\sigma$ -closed subgroup of  $\mathcal{G} \times \mathcal{H}$  and the claim reduces to the similar formula for algebraic groups.  $\square$

## 4 Finiteness theorems

There is no direct difference analog of Hilbert's basis theorem: There exist infinite strictly ascending chains of difference ideals in the  $\sigma$ -polynomial ring  $k\{y_1, \dots, y_n\}$ . (See [Coh65, Example 3, p. 73].) The Ritt–Raudenbush basis theorem in difference algebra ([RR39] or [Lev08, Theorem 2.5.11]) only asserts that every ascending chain of perfect difference ideals in  $k\{y_1, \dots, y_n\}$  is finite. However, in our group theoretic setup the situation is better behaved. Indeed, in this section we will prove two important finiteness theorems. Let  $A$  be a finitely  $\sigma$ -generated  $k$ - $\sigma$ -Hopf algebra. The first finiteness theorem (Theorem 4.1) asserts that every  $\sigma$ -Hopf ideal of  $A$  is finitely generated as a  $\sigma$ -ideal. The second finiteness theorem (Theorem 4.5) asserts that every  $k$ - $\sigma$ -Hopf subalgebra of  $A$  is finitely  $\sigma$ -generated over  $k$ . In Section 9 we will prove a third finiteness theorem (Theorem 9.1): The set of minimal prime  $\sigma$ -ideals of  $A$  is finite.

**Theorem 4.1.** *Let  $H$  be  $\sigma$ -algebraic group and  $G \leq H$  a  $\sigma$ -closed subgroup. Then the defining ideal  $\mathbb{I}(G) \subset k\{H\}$  of  $G$  is finitely generated as a  $\sigma$ -ideal.*

*Proof.* We may embed  $H$  as a  $\sigma$ -closed subgroup in some algebraic group  $\mathcal{G}$ . For example, we may choose  $\mathcal{G} = \text{GL}_n$  by Theorem 2.13. If the defining ideal of  $G$  in  $k\{\mathcal{G}\}$  is finitely  $\sigma$ -generated, then also the defining ideal of  $G$  in  $k\{H\} = k\{G\}/\mathbb{I}(H)$  is finitely  $\sigma$ -generated. We can therefore assume that  $H = \mathcal{G}$ .

As in Section 3 let  $\mathcal{G}_i$  denote the kernel of the projection  $\pi_i: G[i] \twoheadrightarrow G[i-1]$  between the Zariski closures of  $G$  in  $\mathcal{G}$ . By Proposition 3.1 there exists an integer  $m \geq 1$  such that  $\sigma_i: \mathcal{G}_i \rightarrow \sigma(\mathcal{G}_{i-1})$  is

an isomorphism for every  $i > m$ . To prove the theorem we will show that  $\mathbb{I}(G[m]) = \mathbb{I}(G) \cap k[\mathcal{G}[m]]$   $\sigma$ -generates  $\mathbb{I}(G) \subset k\{\mathcal{G}\} = \cup_{i \geq 0} k[\mathcal{G}[i]]$ . To do this it is sufficient to show that

$$\mathbb{I}(G[i]) = (\mathbb{I}(G[i-1]), \sigma(\mathbb{I}(G[i-1]))) \subset k[\mathcal{G}[i]] \quad (6)$$

for  $i > m$ . The ideal to the right-hand side of (6) defines an algebraic group

$$\mathcal{H}_i = (G[i-1] \times {}^\sigma \mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(G[i-1])) \leq \mathcal{G}[i] = \mathcal{G} \times {}^\sigma \mathcal{G} \times \cdots \times {}^\sigma \mathcal{G}.$$

Clearly  $G[i] \leq \mathcal{H}_i$  and the projection  $\pi_i: \mathcal{H}_i \rightarrow G[i-1]$  is surjective<sup>1</sup>. The kernel of  $\pi_i: \mathcal{H}_i \rightarrow G[i-1]$  is  $1 \times {}^\sigma(\mathcal{G}_{i-1})$ . Since  $i > m$  we have  $1 \times {}^\sigma(\mathcal{G}_{i-1}) = \mathcal{G}_i$ . Thus the downwards arrows in the commutative diagram

$$\begin{array}{ccc} G[i] & \xrightarrow{\quad} & \mathcal{H}_i \\ & \searrow \pi_i & \swarrow \pi_i \\ & G[i-1] & \end{array}$$

have the same kernel. This implies that  $G[i] = \mathcal{H}_i$  and identity (6) is proved.  $\square$

We have actually proved a slightly stronger statement which we record for later use.

**Corollary 4.2.** *Let  $\mathcal{G}$  be an algebraic group and  $G \leq \mathcal{G}$  a  $\sigma$ -closed subgroup. For  $i \geq 0$  let  $G[i]$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}$ . Then there exists an integer  $m \geq 0$  such that  $\mathbb{I}(G[i]) = (\mathbb{I}(G[i-1]), \sigma(\mathbb{I}(G[i-1])))$  for  $i > m$ , i.e.,  $G[i] = (G[i-1] \times {}^\sigma \mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(G[i-1]))$ .  $\square$*

**Corollary 4.3.** *Every descending chain of  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group is finite.*

*Proof.* A descending chain  $H_1 \geq H_2 \geq \cdots$  of  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G$  corresponds to an ascending chain  $\mathbb{I}(H_1) \subset \mathbb{I}(H_2) \subset \cdots$  of  $\sigma$ -Hopf ideals in  $k\{G\}$ . By Theorem 4.1 the union  $\bigcup \mathbb{I}(H_i)$  (which corresponds to the intersection  $\bigcap H_i$ ) is finitely generated as a  $\sigma$ -ideal. Thus there exists an integer  $n \geq 1$  such that  $\bigcup \mathbb{I}(H_i) = \mathbb{I}(H_n)$ . Then  $H_n = H_{n+1} = \cdots$ .  $\square$

To prove the second finiteness theorem we need a simple lemma on  $k$ - $\sigma$ -Hopf algebras.

**Lemma 4.4.** *Let  $A$  be a  $k$ - $\sigma$ -Hopf algebra. Then every finite subset of  $A$  is contained in a finitely  $\sigma$ -generated  $k$ - $\sigma$ -Hopf subalgebra.*

*Proof.* By [Wat79, Section 3.3] a finite subset of  $A$  is contained in a Hopf subalgebra  $B$  which is finitely generated as a  $k$ -algebra. Then  $k\{B\} \subset A$  is finitely  $\sigma$ -generated over  $k$  and since the comultiplication and the antipode are  $\sigma$ -morphisms,  $k\{B\}$  is a Hopf subalgebra.  $\square$

**Theorem 4.5.** *Let  $A$  be a  $k$ - $\sigma$ -Hopf algebra which is finitely  $\sigma$ -generated over  $k$  and  $B \subset A$  a  $k$ - $\sigma$ -Hopf subalgebra. Then  $B$  is finitely  $\sigma$ -generated over  $k$ .*

*Proof.* For a Hopf subalgebra  $C$  of  $A$  let  $\mathfrak{m}_C \subset C$  denote the kernel of the counit  $\varepsilon: C \rightarrow k$ . The ideal  $(\mathfrak{m}_B) \subset A$  is a  $\sigma$ -Hopf ideal. By Theorem 4.1 it is finitely  $\sigma$ -generated. So there exists a finite set  $F \subset \mathfrak{m}_B$  such that  $[F] = (\mathfrak{m}_B)$ . By Lemma 4.4 there exists a finitely  $\sigma$ -generated  $k$ - $\sigma$ -Hopf subalgebra  $C$  of  $B$  containing  $F$ . Then  $(\mathfrak{m}_C) = (\mathfrak{m}_B)$ . By Corollary 3.10 in [Tak72] the mapping  $C \mapsto (\mathfrak{m}_C)$  from Hopf subalgebras to Hopf ideals is injective. Thus  $B = C$  is finitely  $\sigma$ -generated over  $k$ .  $\square$

As an application of Corollary 4.2, we will prove a dimension theorem, which will then be used in Section 12 in the proof of an analog of the Jordan–Hölder theorem. A dimension theorem for differential algebraic groups has been proved in [Sit74]. It is interesting to note that the dimension theorem fails for difference varieties. See [Coh65, Chapter 8, Section 8]. However, it holds for  $\sigma$ -algebraic groups:

**Theorem 4.6.** *Let  $H_1$  and  $H_2$  be  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G$ . Then*

$$\sigma\text{-dim}(H_1 \cap H_2) + \sigma\text{-dim}(G) \geq \sigma\text{-dim}(H_1) + \sigma\text{-dim}(H_2) \quad (7)$$

and

$$\text{ord}(H_1 \cap H_2) + \text{ord}(G) \geq \text{ord}(H_1) + \text{ord}(H_2). \quad (8)$$

<sup>1</sup>A morphism  $\mathcal{G} \rightarrow \mathcal{H}$  of algebraic groups, i.e., affine group schemes of finite type over  $k$  is surjective if the dual map  $k[\mathcal{H}] \rightarrow k[\mathcal{G}]$  is injective. See [Mil12, Chapter VII, Section 7] for more details.



*Proof.* Let  $\mathcal{G}$  be an algebraic group containing  $G$  as a  $\sigma$ -closed subgroup. We consider the Zariski closures inside  $\mathcal{G}$ . By Corollary 4.2 there exists an integer  $m \geq 0$  such that

$$\mathbb{I}((H_1 \cap H_2)[i]) = (\mathbb{I}((H_1 \cap H_2)[i-1]), \sigma(\mathbb{I}((H_1 \cap H_2)[i-1])))$$

for  $i > m$ . Since  $\mathbb{I}(H_1 \cap H_2) = \mathbb{I}(H_1) + \mathbb{I}(H_2)$  there exists  $n \geq m$  such that

$$\mathbb{I}((H_1 \cap H_2)[m]) \subset \mathbb{I}(H_1[n]) + \mathbb{I}(H_2[n]) = \mathbb{I}(H_1[n] \cap H_2[n]).$$

But then

$$\mathbb{I}((H_1 \cap H_2)[m+i]) \subset \mathbb{I}(H_1[n+i] \cap H_2[n+i]) \quad (9)$$

for every  $i \geq 0$  and so

$$H_1[n+i] \cap H_2[n+i] \leq (H_1 \cap H_2)[m+i] \times \sigma^{m+i+1}\mathcal{G} \times \cdots \times \sigma^{n+i}\mathcal{G}.$$

Therefore

$$\dim(H_1[n+i] \cap H_2[n+i]) \leq \dim((H_1 \cap H_2)[m+i]) + (n-m) \dim(\mathcal{G})$$

and so

$$\begin{aligned} \dim((H_1 \cap H_2)[m+i]) &\geq \dim(H_1[n+i] \cap H_2[n+i]) - (n-m) \dim(\mathcal{G}) \\ &\geq \dim(H_1[n+i]) + \dim(H_2[n+i]) - \dim(G[n+i]) - (n-m) \dim(\mathcal{G}). \end{aligned}$$

Now using Theorem 3.5 and comparing the coefficients of  $i$  yields identity (7).

It remains to prove (8). Obviously this is true if  $\text{ord}(G) = \infty$ . So we can assume  $\text{ord}(G) < \infty$ , i.e.,  $\sigma\text{-dim}(G) = 0$ . Note that (9) implies that the intersection of  $\mathbb{I}(H_1[n+i] \cap H_2[n+i])$  with  $k[\mathcal{G}[m+i]]$  equals  $\mathbb{I}((H_1 \cap H_2)[m+i])$ . This means that the morphism of algebraic groups

$$\phi: H_1[n+i] \cap H_2[n+i] \rightarrow (H_1 \cap H_2)[m+i]$$

induced from the projection  $\mathcal{G} \times \sigma\mathcal{G} \times \cdots \times \sigma^{n+i}\mathcal{G} \rightarrow \mathcal{G} \times \sigma\mathcal{G} \times \cdots \times \sigma^{m+i}\mathcal{G}$  is surjective. Since  $\sigma\text{-dim}(H_1) = 0$ , the kernel of the projections  $H_1[n+i] \twoheadrightarrow H_1[m+i]$  is finite for  $i \gg 0$ . Therefore also  $\phi$  has finite kernel and it follows that for  $i \gg 0$

$$\begin{aligned} \text{ord}(H_1 \cap H_2) &= \dim((H_1 \cap H_2)[m+i]) = \dim(H_1[n+i] \cap H_2[n+i]) \\ &\geq \dim(H_1[n+i]) + \dim(H_2[n+i]) - \dim(G[n+i]) \\ &= \text{ord}(H_1) + \text{ord}(H_2) - \text{ord}(G). \end{aligned}$$

□

## 5 Representations of difference algebraic groups

In this section we present an application of the first finiteness theorem (Theorem 4.1). We prove the difference analog of a theorem of Chevalley for algebraic groups. Namely, we show that every  $\sigma$ -closed subgroup of a  $\sigma$ -algebraic group can be realized as the stabilizer of a line. We also show that the category of representations of  $\mathbb{G}_m^n$  as a difference algebraic group is semi-simple.

Categories of representations of  $\sigma$ -algebraic groups have been studied in [OWb]. There the authors introduce  $\sigma$ -tannakian categories, which provide a purely categorical characterization of those categories, which are the category of representations of a  $\sigma$ -algebraic group. We plan to explore the relation between properties of a  $\sigma$ -algebraic group and properties of its category of representations in a future work.

**Definition 5.1.** *Let  $G$  be a  $\sigma$ -algebraic group. A representation of  $G$  is a pair  $(V, \phi)$  comprising a finite dimensional  $k$ -vector space  $V$  and a morphism  $\phi: G \rightarrow \text{GL}(V)$  of  $\sigma$ -algebraic groups. The representation is called faithful if  $\phi$  is a  $\sigma$ -closed embedding.*

We will often omit  $\phi$  from the notation. A morphism  $(V, \phi) \rightarrow (V', \phi')$  of representations of  $G$  is a  $k$ -linear map  $f: V \rightarrow V'$  which is  $G$ -equivariant, i.e.,

$$\begin{array}{ccc} V \otimes_k R & \xrightarrow{f \otimes R} & V' \otimes_k R \\ \phi(g) \downarrow & & \downarrow \phi'(g) \\ V \otimes_k R & \xrightarrow{f \otimes R} & V' \otimes_k R \end{array}$$

commutes for every  $g \in G(R)$  and any  $k$ - $\sigma$ -algebra  $R$ .

**Lemma 5.2.** *Let  $G$  be a  $\sigma$ -algebraic group. The category of representations of  $G$  is equivalent to the category of finite dimensional comodules over  $k\{G\}$ .*

*Proof.* This is similar to Section 3.2 in [Wat79].  $\square$

**Lemma 5.3.** *Let  $V$  be a representation of the  $\sigma$ -algebraic group  $G$  and  $W \leq V$  a linear subspace. Then the stabilizer  $G_W$  of  $W$ , defined by*

$$G_W(R) = \{g \in G(R) \mid g(W \otimes_k R) \subset W \otimes_k R\}$$

*for any  $k$ - $\sigma$ -algebra  $R$ , is a  $\sigma$ -closed subgroup of  $G$ .*

*Proof.* Let  $v_1, \dots, v_n$  be a basis of  $V$  such that  $v_1, \dots, v_m$  is a basis of  $W$ . Let  $\rho: V \rightarrow V \otimes_k k\{G\}$  denote the comodule structure corresponding to the given representation and write  $\rho(v_j) = \sum_{i=1}^n v_i \otimes a_{ij} \in V \otimes_k k\{G\}$  for  $j = 1, \dots, n$ . So for a  $k$ - $\sigma$ -algebra  $R$  and  $g \in G(R) = \text{Hom}(k\{G\}, R)$  we have  $g(v_j \otimes 1) = \sum_{i=1}^n v_i \otimes g(a_{ij}) \in V \otimes_k R$ . This shows the  $g \in G_W(R)$  if and only if  $g(a_{ij}) = 0$  for  $j = 1, \dots, m$  and  $i = m+1, \dots, n$ . Thus

$$G_W = \mathbb{V}([a_{ij} \mid 1 \leq j \leq m, m+1 \leq i \leq n]).$$

$\square$

We know from Theorem 2.13 that every  $\sigma$ -algebraic group admits a faithful representation. The following theorem provides a strengthening of this result:

**Theorem 5.4.** *Let  $G$  a  $\sigma$ -algebraic group and  $H \leq G$  a  $\sigma$ -closed subgroup. Then there exists a faithful representation  $V$  of  $G$  and a line  $L \leq V$  (i.e., a one dimensional  $k$ -subspace) such that  $H$  is the stabilizer of  $L$ , i.e.,*

$$H(R) = \{g \in G(R) \mid g(L \otimes_k R) \subset L \otimes_k R\}$$

*for any  $k$ - $\sigma$ -algebra  $R$ .*

*Proof.* We will first construct a representation  $V$  of  $G$  such that  $H$  is the stabilizer of a subspace  $W$  of  $V$ . By Theorem 4.1 there exists a finite set  $F \subset \mathbb{I}(H) \subset k\{G\}$  such that  $\mathbb{I}(H) = [F]$ . By Section 3.3 in [Wat79] there exists a finite dimensional subcomodule  $V$  of  $k\{G\}$  such that  $F \subset V$ . Let  $W = V \cap \mathbb{I}(H) \leq V$ . If  $v_1, \dots, v_n$  is a basis of  $V$  such that  $v_1, \dots, v_m$  is a basis of  $W$  and  $\Delta(v_j) = \sum_{i=1}^n v_i \otimes a_{ij} \in V \otimes_k k\{G\}$  for  $j = 1, \dots, n$ , then

$$\mathbb{I}(G_W) = [a_{ij} \mid 1 \leq j \leq m, m+1 \leq i \leq n]$$

by the proof of Lemma 5.3. Since  $\mathbb{I}(H)$  and  $V$  are  $k\{H\}$ -comodules also  $W = \mathbb{I}(H) \cap V$  is a  $k\{H\}$ -comodule. So  $W$  is stable under  $H$ , i.e.,  $H \leq G_W$ , or  $\mathbb{I}(G_W) \subset \mathbb{I}(H)$ . We have

$$v_j = \sum_{i=1}^n \varepsilon(v_i) a_{ij} = \sum_{i=m+1}^n \varepsilon(v_i) a_{ij},$$

since  $\varepsilon(\mathbb{I}(H)) = 0$ . This shows that every  $f \in F \subset W$  lies in  $[a_{ij} \mid 1 \leq j \leq m, m+1 \leq i \leq n] = \mathbb{I}(G_W)$ . Therefore  $\mathbb{I}(H) = [F] \subset \mathbb{I}(G_W)$  and consequently  $H = G_W$ .

Now the  $m$ -th exterior power  $\wedge^m V$  is naturally a representation of  $G$  and  $L = \wedge^m W \leq \wedge^m V$  is one dimensional. Moreover  $G_L = G_W$ . (See Section A.2 in [Wat79].) In case  $\wedge^m V$  is not faithful, we can replace it by  $\wedge^m V \oplus V'$ , where  $V'$  is a faithful representation of  $G$ .  $\square$

An algebraic group  $\mathcal{G}$  over a field of characteristic zero is reductive if and only if it is linearly reductive, i.e., every representation of  $\mathcal{G}$  is a direct sum of irreducible representations. In differential algebra, the only linearly reductive linear differential algebraic groups are those which are the constant points of a reductive algebraic group ([MO11, Theorem 3.14]). In particular, the linear differential algebraic group  $\mathbb{G}_m$  is not linearly reductive. Indeed, the representation

$$\mathbb{G}_m \rightarrow \text{GL}_2, \quad g \mapsto \begin{pmatrix} g & \delta(g) \\ 0 & g \end{pmatrix}$$

is not semi-simple. For difference algebraic groups the situation is fundamentally different. We show here that tori are linearly reductive difference algebraic groups and leave the characterization of the linearly reductive difference algebraic groups for the future.

**Theorem 5.5.** *Every representation of the difference algebraic group  $G = \mathbb{G}_m^n$  is a direct sum of one-dimensional representations.*

*Proof.* Let us denote by  $X$  the set of all elements of  $k\{G\} = k\{y_1, y_1^{-1}, \dots, y_n, y_n^{-1}\}$  which are products of elements of the form  $\sigma^\alpha(y_i)^\beta$  where  $\alpha \in \mathbb{N}$ ,  $\beta \in \mathbb{Z}$  and  $1 \leq i \leq n$ . Then  $X$  is a  $k$ -basis of  $k\{G\}$  and every element  $\chi \in X$  is group-like, i.e.,  $\Delta(\chi) = \chi \otimes \chi$  and  $\varepsilon(\chi) = 1$  where  $\Delta: k\{G\} \rightarrow k\{G\} \otimes_k k\{G\}$  is the comultiplication and  $\varepsilon: k\{G\} \rightarrow k$  the counit.

Let  $V$  be a representation of  $G$ ,  $\rho: V \rightarrow V \otimes_k k\{G\}$  the corresponding comodule and  $v \in V$ . Then we can write

$$\rho(v) = \sum_{\chi \in X} a_\chi \otimes \chi, \quad a_\chi \in V.$$

Applying the comodule identities  $(\text{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \text{id}_{k\{G\}}) \circ \rho$  and  $(\text{id}_V \otimes \varepsilon) \circ \rho = \text{id}_V$  (see [Wat79, Section 3.2]) to  $v$ , we find that

$$\sum_{\chi \in X} a_\chi \otimes \chi \otimes \chi = \sum_{\chi \in X} \rho(a_\chi) \otimes \chi, \quad \text{and} \quad (10)$$

$$v = \sum_{\chi \in X} a_\chi. \quad (11)$$

Identity (10) implies that  $\rho(a_\chi) = a_\chi \otimes \chi$ . So  $g(a_\chi \otimes 1) = a_\chi \otimes g(\chi)$  for  $g \in G(R) = \text{Hom}(k\{G\}, R)$  and  $R$  a  $k$ - $\sigma$ -algebra. Thus  $ka_\chi$  is a subrepresentation of  $V$  and it follows from (11) that  $V$  is spanned by all the one-dimensional subrepresentations arising in this way.  $\square$

## 6 The limit degree

In this section we introduce an important numerical invariant for  $\sigma$ -algebraic groups (of  $\sigma$ -dimension zero) called the limit degree. We also show that the category of algebraic  $\sigma$ -groups introduced and studied in [KP07] is equivalent to the category of  $\sigma$ -algebraic groups of  $\sigma$ -dimension zero and limit degree one.

By the *size*  $|\mathcal{G}|$  of an algebraic group  $\mathcal{G}$  we mean the dimension of  $k[\mathcal{G}]$  as a  $k$ -vector space. So the size is either a non-negative integer or  $\infty$ . In the sequel we will employ the usual rules for calculating with the symbol  $\infty$ . If  $\mathcal{G}_1 \xrightarrow{\phi_1} \mathcal{G}_2 \xrightarrow{\phi_2} \mathcal{G}_3$  are surjective morphisms of algebraic groups, then

$$|\ker(\phi_2 \circ \phi_1)| = |\ker(\phi_2)| \cdot |\ker(\phi_1)|. \quad (12)$$

**Proposition 6.1.** *Let  $G$  be a  $\sigma$ -algebraic group and  $G \hookrightarrow \mathcal{G}$  a  $\sigma$ -closed embedding. Then the size of the growth group of  $G$  with respect to the embedding  $G \hookrightarrow \mathcal{G}$  does not depend on the choice of  $\mathcal{G}$  and the  $\sigma$ -closed embedding.*

*Proof.* For  $i \geq 0$  let  $G[i]$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}$  and  $\mathcal{G}_i$  the kernel of the projection  $\pi_i: G[i] \rightarrow G[i-1]$ . By Proposition 3.1 the integer  $d = |\mathcal{G}_i|$  does not depend on  $i$  for  $i \gg 0$ . Let  $a = (a_1, \dots, a_n)$  generate  $k[G[0]] \subset k\{G\}$  as a  $k$ -algebra. Then  $a$  generates  $k\{G\}$  as a  $k$ - $\sigma$ -algebra.

Let  $\mathcal{G}'$  be another algebraic group and  $G \hookrightarrow \mathcal{G}'$  a  $\sigma$ -closed embedding. Let  $G'[i]'$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}'$  and let  $d'$  and  $a'$  be as above. We have to show that  $d = d'$ .

Since  $a$ , as well as  $a'$ ,  $\sigma$ -generate  $k\{G\}$ , there exists an integer  $m \geq 1$  such that  $a' \in k[a, \dots, \sigma^m(a)]$  and  $a \in k[a', \dots, \sigma^m(a')]$ . Then, for  $i \geq 0$ , we have  $k[a', \dots, \sigma^i(a')] \subset k[a, \dots, \sigma^{m+i}(a)]$  and  $k[a, \dots, \sigma^i(a)] \subset k[a', \dots, \sigma^{m+i}(a')]$ . So for  $j \geq m$ :

$$k[a, \dots, \sigma^i(a)] \subset k[a', \dots, \sigma^{m+i}(a')] \subset k[a', \dots, \sigma^{j+i}(a')] \subset k[a, \dots, \sigma^{m+j+i}(a)].$$

These inclusions of Hopf algebras correspond to surjective morphisms of algebraic groups

$$G[m+j+i] \twoheadrightarrow G[j+i]' \twoheadrightarrow G[m+i]' \twoheadrightarrow G[i].$$

We have  $|\ker(G[m+j+i] \twoheadrightarrow G[i])| \geq |\ker(G[j+i]' \twoheadrightarrow G[m+i]')|$  by (12). But by (12) and Proposition 3.1 we also have  $|\ker(G[m+j+i] \twoheadrightarrow G[i])| = d^{m+j}$  and  $|\ker(G[j+i]' \twoheadrightarrow G[m+i]')| = d'^{j-m}$  for  $i \gg 0$ . Consequently,  $d^{m+j} \geq d'^{j-m}$ . Letting  $j$  tend to infinity, we find  $d \geq d'$ . By symmetry,  $d = d'$ .  $\square$

**Definition 6.2.** Let  $G$  be a  $\sigma$ -algebraic group. Choose an algebraic group  $\mathcal{G}$  and a  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ . The size of the growth group of  $G$  with respect to the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$  is called the limit degree of  $G$  and is denoted by

$$\text{ld}(G).$$

By Proposition 6.1 the limit degree of  $G$  does not depend on the choice of  $\mathcal{G}$  and the  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$ .

The expression “limit degree” is motivated by the fact that

$$\text{ld}(G) = \lim_{i \rightarrow \infty} \deg(\pi_i),$$

where  $\deg(\pi_i)$  denotes the degree of the projection  $\pi_i: G[i] \rightarrow G[i-1]$ . The naming is also motivated by Proposition 6.6 and Theorem 13.1.

**Remark 6.3.** By Corollary 3.9 the limit degree of a  $\sigma$ -algebraic group is finite if and only if it has  $\sigma$ -dimension zero.

**Example 6.4.** Let  $0 \leq \alpha_1 < \dots < \alpha_n$  and  $1 \leq \beta_1, \dots, \beta_n$  be integers and  $G \leq \mathbb{G}_m$  the  $\sigma$ -closed subgroup of the multiplicative group  $\mathbb{G}_m$  given by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\}$$

for every  $k$ - $\sigma$ -algebra  $R$ . Then  $\text{ld}(G) = \beta_n$  by Example 3.3.

**Example 6.5.** Let  $\mathcal{G}$  be an algebraic group. Then  $\text{ld}([\sigma]_k \mathcal{G}) = |\mathcal{G}|$ . This follows from the fact that the growth group of  $[\sigma]_k \mathcal{G}$  with respect to the tautological  $\sigma$ -closed embedding  $[\sigma]_k \mathcal{G} \hookrightarrow \mathcal{G}$  is  $\mathcal{G}$ .

Let  $K|k$  be an extension of  $\sigma$ -fields. Assume that there exists a finite set  $B \subset K$  such that  $B, \sigma(B), \dots$  generates  $K$  as a field extension of  $k$ , then the limit degree  $\text{ld}(K|k)$  is the limit  $\lim_{i \rightarrow \infty} d_i$ , where  $d_i$  is the degree of the field extension  $k(B, \dots, \sigma^i(B))|k(B, \dots, \sigma^{i-1}(B))$ . The limit exists and does not depend on the choice of  $B$  ([Lev08, Section 4.3]). The following proposition shows that our definition of the limit degree generalizes the classical definition ([Lev08, p. 394]) of the limit degree (for irreducible difference varieties in the sense of [Coh65] and [Lev08]).

**Proposition 6.6.** Let  $G$  be a  $\sigma$ -algebraic group. If  $G$  is  $\sigma$ -integral (i.e.,  $k\{G\}$  is an integral domain and  $\sigma: k\{G\} \rightarrow k\{G\}$  is injective), then the limit degree of  $G$  equals the limit degree of the field of fractions of  $k\{G\}$  over  $k$ .

*Proof.* Let  $\mathcal{G}$  be an algebraic group containing  $G$  as a  $\sigma$ -closed subgroup. For  $i \geq 0$  let  $G[i]$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}$  and let  $B \subset k[G[0]]$  be a finite set which generates  $k[G[0]] \subset k\{G\}$  as a  $k$ -algebra. Let  $K$  denote the field of fractions of  $k\{G\}$ . Then  $B, \sigma(B), \dots$  generates  $K$  as a field extension of  $k$  and  $k(B, \sigma(B), \dots, \sigma^i(B))$  is the field of fractions of  $k[G[i]]$ . Therefore the degree of the field extension  $k(B, \dots, \sigma^i(B))|k(B, \dots, \sigma^{i-1}(B))$  equals the degree of the projection  $G[i] \rightarrow G[i-1]$ .  $\square$

Our next aim is to characterize the algebraic  $\sigma$ -groups introduced in [KP07] within the category of  $\sigma$ -algebraic groups.

**Proposition 6.7.** Let  $G$  be a  $\sigma$ -algebraic group. Then  $\text{ld}(G) = 1$  if and only if  $k\{G\}$  is finitely generated as a  $k$ -algebra.

*Proof.* Fix a  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$  and let  $G[i]$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathcal{G}$ . So  $k\{G\} = \cup_{i \geq 0} k[G[i]]$ . If  $\text{ld}(G) = 1$  there exists an integer  $m \geq 0$  such that  $\pi_i: G[i] \rightarrow G[i-1]$  has trivial kernel for  $i > m$ , so  $\pi_i$  is an isomorphism and therefore  $k[G[i]] = k[G[i-1]]$ . Consequently,  $k\{G\} = k[G[m]]$  is finitely generated as a  $k$ -algebra.

Conversely, if  $k\{G\}$  is a finitely generated  $k$ -algebra, we can consider the algebraic group  $\mathcal{G}$  associated with the Hopf algebra  $k\{G\}^\#$ . So  $k[\mathcal{G}] = k\{G\}^\#$ . Let  $R$  be a  $k$ - $\sigma$ -algebra. Since  $G(R) = \text{Hom}(k\{G\}, R)$  is a subgroup of

$$\text{Hom}(k\{G\}^\#, R^\#) = \mathcal{G}(R^\#) = ([\sigma]_k \mathcal{G})(R) = \text{Hom}(k\{\mathcal{G}\}, R)$$

the morphism  $k\{\mathcal{G}\} \rightarrow k\{G\}$  of  $k$ - $\sigma$ -algebras induced by Lemma 1.7 is a morphism of  $k$ - $\sigma$ -Hopf algebras. With respect to the corresponding  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$  we have  $k\{G\} = k[G[0]] = k[G[1]] = \dots$  and therefore the associated growth group is trivial. Thus  $\text{ld}(G) = 1$ .  $\square$

Let us now recall the definition of algebraic  $\sigma$ -groups from [KP07]. We start by introducing algebraic  $\sigma$ -varieties. Let  $k$  be a  $\sigma$ -field and  $\mathcal{X}$  a variety over  $k$ , where, for our purposes, a variety over  $k$  is an affine scheme of finite type over  $k$ . As in Section 1.4 let  ${}^\sigma\mathcal{X}$  denote the variety over  $k$  obtained from  $\mathcal{X}$  by base extension via  $\sigma: k \rightarrow k$ . Similarly, if  $\phi: \mathcal{X} \rightarrow \mathcal{Y}$  is a morphism of varieties over  $k$ , then  ${}^\sigma\phi: {}^\sigma\mathcal{X} \rightarrow {}^\sigma\mathcal{Y}$  is the morphism obtained from  $\phi$  by base extension via  $\sigma: k \rightarrow k$ .

An *algebraic  $\sigma$ -variety* over  $k$  is a variety  $\mathcal{X}$  over  $k$  together with a morphism  $\tilde{\sigma}: \mathcal{X} \rightarrow {}^\sigma\mathcal{X}$  of varieties over  $k$ . A morphism between algebraic  $\sigma$ -varieties is a morphism  $\phi: \mathcal{X} \rightarrow \mathcal{Y}$  of varieties such that

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\tilde{\sigma}} & {}^\sigma\mathcal{X} \\ \phi \downarrow & & \downarrow {}^\sigma\phi \\ \mathcal{Y} & \xrightarrow{\tilde{\sigma}} & {}^\sigma\mathcal{Y} \end{array}$$

commutes. An *algebraic  $\sigma$ -group* is a group object in the category of algebraic  $\sigma$ -varieties. Equivalently, an algebraic  $\sigma$ -group is an algebraic group  $\mathcal{G}$  over  $k$  together with a morphism  $\tilde{\sigma}: \mathcal{G} \rightarrow {}^\sigma\mathcal{G}$  of algebraic groups.

**Theorem 6.8.** *The category of algebraic  $\sigma$ -groups is equivalent to the category of  $\sigma$ -algebraic groups of  $\sigma$ -dimension zero and limit degree one.*

*Proof.* Let  $R$  be a  $k$ -algebra. To define a  $k$ - $\sigma$ -algebra structure on  $R$  is equivalent to defining a morphism of  $k$ -algebras  $\bar{\sigma}: {}^\sigma R \rightarrow R$ . Given  $\sigma: R \rightarrow R$ , we can define  $\bar{\sigma}: {}^\sigma R \rightarrow R$ ,  $r \otimes \lambda \mapsto \sigma(r)\lambda$ . Conversely, given  $\bar{\sigma}: {}^\sigma R \rightarrow R$ , we can define  $\sigma: R \xrightarrow{\text{id} \otimes 1} R \otimes_k k = {}^\sigma R \xrightarrow{\bar{\sigma}} R$ . Moreover, if  $R$  and  $S$  are  $k$ - $\sigma$ -algebras and  $\psi: R \rightarrow S$  is a morphism of  $k$ -algebras, then  $\psi$  is a morphism of  $k$ - $\sigma$ -algebras if and only if

$$\begin{array}{ccc} {}^\sigma R & \xrightarrow{\bar{\sigma}} & R \\ {}^\sigma\psi \downarrow & & \downarrow \psi \\ {}^\sigma S & \xrightarrow{\bar{\sigma}} & S \end{array}$$

commutes.

Dualizing the definition, an algebraic  $\sigma$ -group  $\mathcal{G}$  corresponds to a finitely generated Hopf algebra  $k[\mathcal{G}]$  together with a morphism of Hopf algebras  $\bar{\sigma} = (\tilde{\sigma})^*: {}^\sigma(k[\mathcal{G}]) \rightarrow k[\mathcal{G}]$ . By the remark from the beginning of the proof, the statement that  $\bar{\sigma}$  is a morphism of Hopf algebras corresponds to the statement that  $k[\mathcal{G}]$  is a  $k$ - $\sigma$ -Hopf algebra. Thus the category of algebraic  $\sigma$ -groups is anti-equivalent to the category of  $k$ - $\sigma$ -Hopf algebras, which are finitely generated over  $k$ . Now the claim follows from Proposition 2.3 and Proposition 6.7.  $\square$

## 7 Quotients

The first goal in this section is to establish the existence of the quotient  $G/N$ , where  $N$  is a normal  $\sigma$ -closed subgroup of a  $\sigma$ -algebraic group  $G$ . We do not address the (highly non-trivial) question of the existence of the quotient  $G/H$  where  $H$  is an arbitrary  $\sigma$ -closed subgroup. As for (affine) algebraic groups, the quotient  $G/H$  will in general not be affine (but rather quasi-projective). For algebraic groups, the analog of Theorem 5.4 is a crucial ingredient for constructing the quotient as a quasi-projective variety. Therefore Theorem 5.4 already gives some indication that “ $G/H$  is a quasi-projective  $\sigma$ -variety”. But to even make sense of this statement, one would need to introduce a substantially heavier foundation of difference algebraic geometry than we have done in Section 1, where we only deal with the affine setting.

We also show how to compute  $\sigma\text{-dim}(G/N)$ ,  $\text{ord}(G/N)$  and  $\text{ld}(G/N)$  from the corresponding values for  $G$  and  $N$ .

Let  $G$  be a  $\sigma$ -algebraic. A  $\sigma$ -closed subgroup  $N \leq G$  is called *normal* if  $N(R)$  is a normal subgroup of  $G(R)$  for any  $k$ - $\sigma$ -algebra  $R$ . We write  $N \trianglelefteq G$  to express that  $N$  is a normal  $\sigma$ -closed subgroup of  $G$ .

If  $\phi: G \rightarrow H$  is a morphism of  $\sigma$ -algebraic groups, we define the kernel of  $\phi$

$$\ker(\phi)$$

to be the subfunctor of  $G$  given by  $R \rightsquigarrow \ker(\phi_R)$ . Then  $\ker(\phi)$  is a normal  $\sigma$ -closed subgroup of  $G$ . Indeed  $\ker(\phi) = \phi^{-1}(1)$ , where  $1 \leq H$  is the trivial  $\sigma$ -closed subgroup of  $H$  defined by the kernel  $\mathfrak{m}_{k\{H\}}$  of the counit  $k\{H\} \rightarrow k$ .

**Definition 7.1.** Let  $G$  be a  $\sigma$ -algebraic group and  $N \trianglelefteq G$  a normal  $\sigma$ -closed subgroup. A morphism of  $\sigma$ -algebraic groups  $\pi: G \rightarrow G/N$  such that  $N \subset \ker(\pi)$  is called a quotient of  $G \bmod N$  if it is universal among such maps, i.e., for every morphism of  $\sigma$ -algebraic groups  $\phi: G \rightarrow H$  with  $N \subset \ker(\phi)$  there exists a unique morphism of  $\sigma$ -algebraic groups  $\phi': G/N \rightarrow H$  such that

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow \phi & \swarrow \phi' \\ & H & \end{array}$$

commutes.

Of course, if a quotient of  $G \bmod N$  exists, it is unique up to a unique isomorphism. We will therefore usually speak of *the* quotient of  $G \bmod N$ .

For affine group schemes over a field (not necessarily of finite type), the fundamental theorem on quotients can be formulated in a purely Hopf algebraic manner ([Tak72]). Recall that a Hopf ideal  $\mathfrak{a}$  in a Hopf algebra  $A$  over  $k$  is called *normal* if, using Sweedler notation,

$$\sum f_{(1)} S(f_{(3)}) \otimes f_{(2)} \in A \otimes_k \mathfrak{a}$$

for any  $f \in \mathfrak{a}$ , where  $S$  is the antipode of  $A$ . Normal Hopf ideals in  $A$  correspond to normal closed subgroup schemes ([Tak72, Lemma 5.1]). Similarly, if  $G$  is a  $\sigma$ -algebraic group, then normal  $\sigma$ -Hopf ideals in  $k\{G\}$  correspond to normal  $\sigma$ -closed subgroups of  $G$  (Cf. Lemma 2.4.). For a Hopf algebra  $A$  over  $k$  let us denote the kernel of the counit  $\varepsilon: A \rightarrow k$  by  $\mathfrak{m}_A$ .

**Theorem 7.2** (M. Takeuchi). *Let  $A$  be a Hopf algebra over  $k$  and  $\mathfrak{a} \subset A$  a Hopf ideal. Then  $A(\mathfrak{a}) = \{f \in A \mid \Delta(f) - f \otimes 1 \in A \otimes_k \mathfrak{a}\}$  is a Hopf subalgebra of  $A$  with  $(\mathfrak{m}_{A(\mathfrak{a})}) = \mathfrak{a}$ . Indeed  $A(\mathfrak{a})$  is the unique Hopf subalgebra with this property and the largest Hopf subalgebra with the property that  $(\mathfrak{m}_{A(\mathfrak{a})}) \subset \mathfrak{a}$ .*

*Proof.* By [Tak72, Lemma 4.4]  $A(\mathfrak{a})$  is a Hopf subalgebra. By [Tak72, Lemma 4.7] it is the largest Hopf subalgebra with  $(\mathfrak{m}_{A(\mathfrak{a})}) \subset \mathfrak{a}$ . Finally, by [Tak72, Theorem 4.3] it is the unique Hopf subalgebra with  $(\mathfrak{m}_{A(\mathfrak{a})}) = \mathfrak{a}$ .  $\square$

The existence of the quotient of  $G \bmod N$  can be reduced to Theorem 7.2. A similar approach was taken in [DVHW14, Section A.9]. While the result in [DVHW14] is formulated in a slightly more general setup (there the  $k$ - $\sigma$ -Hopf algebras need not be finitely  $\sigma$ -generated over  $k$ ) the result we prove here is stronger. Indeed, with the aid of the second finiteness theorem (Theorem 4.5) we show that  $G/N$  is  $\sigma$ -algebraic, i.e.,  $k\{G/N\}$  is finitely  $\sigma$ -generated over  $k$ . This question remained open in [DVHW14].

**Theorem 7.3.** *Let  $G$  be a  $\sigma$ -algebraic group and  $N \trianglelefteq G$  a  $\sigma$ -closed subgroup. Then the quotient of  $G \bmod N$  exists. Moreover, a morphism of  $\sigma$ -algebraic groups  $\pi: G \rightarrow G/N$  is the quotient of  $G \bmod N$  if and only if  $\ker(\pi) = N$  and  $\pi^*: k\{G/N\} \rightarrow k\{G\}$  is injective.*

*Proof.* By Theorem 7.2

$$k\{G\}(\mathbb{I}(N)) = \{f \in k\{G\} \mid \Delta(f) - f \otimes 1 \in k\{G\} \otimes_k \mathbb{I}(N)\}$$

is a Hopf subalgebra of  $k\{G\}$ . Clearly it is also a  $k$ - $\sigma$ -Hopf subalgebra. From Theorem 4.5 we know that  $k\{G\}(\mathbb{I}(N))$  is finitely  $\sigma$ -generated over  $k$ . So we can define  $G/N$  as the  $\sigma$ -algebraic group represented by  $k\{G\}(\mathbb{I}(N))$ , i.e.,  $k\{G/N\} = k\{G\}(\mathbb{I}(N))$ . Let  $\pi: G \rightarrow G/N$  be the morphism of  $\sigma$ -algebraic groups corresponding to the inclusion  $k\{G/N\} \subset k\{G\}$  of  $k$ - $\sigma$ -Hopf algebras.

Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups such that  $N \subset \ker(\phi)$ . As  $\ker(\phi) = \mathbb{V}(\phi^*(\mathfrak{m}_{k\{H\}}))$ , the Hopf algebraic meaning of  $N \subset \ker(\phi)$  is  $\phi^*(\mathfrak{m}_{k\{H\}}) \subset \mathbb{I}(N)$ . To show that  $\pi$  has the required universal property, it suffices to show that  $\phi^*(k\{H\}) \subset k\{G/N\}$ . We know from Theorem 7.2 that  $k\{G/N\}$  is the largest Hopf subalgebra of  $k\{G\}$  such that  $\mathfrak{m}_{k\{G/N\}} \subset \mathbb{I}(N)$ . As  $\mathfrak{m}_{\phi^*(k\{H\})} = \phi^*(\mathfrak{m}_{k\{H\}}) \subset \mathbb{I}(N)$  we find  $\phi^*(k\{H\}) \subset k\{G/N\}$ .

Clearly  $\pi^*$  is injective. Moreover,  $\ker(\pi) = \mathbb{V}(\pi^*(\mathfrak{m}_{k\{G/N\}})) = \mathbb{V}(\mathbb{I}(N)) = N$  by Theorem 7.2.

If  $\pi: G \rightarrow G/N$  is a morphism of  $\sigma$ -algebraic groups such that  $N = \ker(\pi)$  and  $\pi^*: k\{G/N\} \rightarrow k\{G\}$  is injective, then  $\pi^*(k\{G/N\})$  is a Hopf subalgebra of  $k\{G\}$  such that  $(\mathfrak{m}_{\pi^*(k\{G/N\})}) = \mathbb{I}(N)$ . Therefore  $\pi^*(k\{G/N\}) = k\{G\}(\mathbb{I}(N))$  by Theorem 7.2.  $\square$

**Corollary 7.4.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups. Then the induced morphism  $G/\ker(\phi) \rightarrow H$  is a  $\sigma$ -closed embedding.*

*Proof.* The Hopf subalgebra  $\phi^*(k\{H\}) \subset k\{G\}$  satisfies  $(\mathfrak{m}_{\phi^*(k\{H\})}) = (\phi^*(\mathfrak{m}_{k\{H\}})) = \mathbb{I}(\ker(\phi))$ . Therefore  $\phi^*(k\{H\}) = k\{G\}(\mathbb{I}(\ker(\phi))) = k\{G/\ker(\phi)\}$  by Theorem 7.2. So  $k\{H\} \rightarrow k\{G/\ker(\phi)\}$  is surjective and  $G/\ker(\phi) \rightarrow H$  is a  $\sigma$ -closed embedding by Lemma 1.6.  $\square$

Let  $\psi: R \rightarrow S$  be a morphism of  $k$ - $\sigma$ -algebras. We say that  $\psi$  is *faithfully flat* if the underlying morphism  $\psi^\sharp: R^\sharp \rightarrow S^\sharp$  of  $k$ -algebras is faithfully flat. In this case, we also say that  $S$  is a faithfully flat  $R$ - $\sigma$ -algebra.

Let  $R$  be a  $k$ - $\sigma$ -algebra and  $\pi: G \rightarrow G/N$  a quotient. As for algebraic groups, the map  $\pi_R: G(R) \rightarrow (G/N)(R)$  need not be surjective in general. (See Example 8.7.) This, at least initially, makes it difficult to transfer constructions familiar from the theory of abstract groups which refer to group elements to  $\sigma$ -algebraic groups. The following lemma is a very useful substitute for the missing surjectivity of  $\pi_R$ . See Section 11, in particular Theorem 11.12 on how this lemma is used.

**Lemma 7.5.** *Let  $G$  be a  $\sigma$ -algebraic group and  $N \trianglelefteq G$  a  $\sigma$ -closed subgroup. Let  $R$  be a  $k$ - $\sigma$ -algebra and  $\bar{g} \in (G/N)(R)$ . Then there exists a faithfully flat morphism  $R \rightarrow S$  of  $k$ - $\sigma$ -algebras and  $g \in G(S)$  such that  $G(S) \rightarrow (G/N)(S)$  maps  $g$  to the image of  $\bar{g}$  in  $(G/N)(S)$ .*

*Proof.* We may use  $\bar{g} \in (G/N)(R) = \text{Hom}(k\{G/N\}, R)$  to form  $S = k\{G\} \otimes_{k\{G/N\}} R$ . Since  $k\{G\}$  is faithfully flat over  $k\{G/N\}$  (See [Wat79, Chapter 14].) it follows that  $R \rightarrow S$ ,  $r \mapsto 1 \otimes r$  is faithfully flat ([Wat79, Section 13.3, p. 105]). Let  $g: k\{G\} \rightarrow S$ ,  $f \mapsto f \otimes 1$ . Then the maps  $k\{G/N\} \xrightarrow{\bar{g}} R \rightarrow S$  and  $k\{G/N\} \rightarrow k\{G\} \xrightarrow{g} S$  are equal. So  $g \in G(S)$  has the required property.  $\square$

Now that we have established the existence of the quotient  $G/N$  we can start to study its properties. To see how the numerical invariants  $\sigma$ -dimension, order and limit degree behave with respect to quotients, we first need to understand how quotients intertwine with Zariski closures.

**Lemma 7.6.** *Let  $\mathcal{G}$  be an algebraic group and  $N \leq G \leq \mathcal{G}$  be  $\sigma$ -closed subgroups. For  $i \geq 0$  let  $G[i]$  and  $N[i]$  denote the  $i$ -th order Zariski closure of  $G$  and  $N$  in  $\mathcal{G}$  respectively. Then  $N$  is normal in  $G$  if and only if  $N[i]$  is normal in  $G[i]$  for every  $i \geq 0$ .*

*Proof.* As  $k\{G\} = \cup_{i \geq 0} k[G[i]]$  is the union of the Hopf subalgebras  $k[G[i]]$ , we see that  $\mathbb{I}(N)$  is a normal Hopf ideal of  $k\{G\}$  if and only if  $\mathbb{I}(N) \cap k[G[i]]$  is a normal Hopf ideal of  $k[G[i]]$  for every  $i \geq 0$ .  $\square$

**Proposition 7.7.** *Let  $\mathcal{G}$  be an algebraic group and  $N \trianglelefteq G \leq \mathcal{G}$ . For  $i \geq 0$  let  $G[i]$  and  $N[i]$  denote the  $i$ -th order Zariski closure of  $G$  and  $N$  in  $\mathcal{G}$  respectively. Then there exists an integer  $m \geq 0$  such that  $G/N$  is a  $\sigma$ -closed subgroup of  $G[m]/N[m]$  and for  $i \geq 0$  the  $i$ -th order Zariski closure of  $G/N$  in  $G[m]/N[m]$  is the quotient of  $G[i+m]$  mod  $N[i+m]$ , i.e.,*

$$(G/N)[i] = G[m+i]/N[m+i].$$

*Proof.* By Theorems 7.2 and 7.3 we have

$$\begin{aligned} k\{G/N\} &= \{f \in k\{G\} \mid \Delta(f) - f \otimes 1 \in k\{G\} \otimes_k \mathbb{I}(N)\} \\ &= \bigcup_{i \geq 0} \{f \in k[G[i]] \mid \Delta(f) - f \otimes 1 \in k[G[i]] \otimes_k \mathbb{I}(N[i])\} \\ &= \bigcup_{i \geq 0} k[G[i]/N[i]]. \end{aligned}$$

Moreover,

$$k[G[i]/N[i]] \subset k[G[i+1]/N[i+1]] \text{ and } \sigma(k[G[i]/N[i]]) \subset k[G[i+1]/N[i+1]].$$

By Corollary 4.2, there exists an integer  $m \geq 0$  such that  $\mathbb{I}(N[j+1]) = (\mathbb{I}(N[j]), \sigma(\mathbb{I}(N[j])))$ , i.e.,  $N[j+1] = (N[j] \times \sigma^j \mathcal{G}) \cap (\mathcal{G} \times \sigma(N[j]))$  for  $j \geq m$ . We claim that

$$k[k[G[m]/N[m]], \dots, \sigma^i(k[G[m]/N[m]))] = k[G[m+i]/N[m+i]] \quad \text{for } i \geq 0. \quad (13)$$

The inclusion “ $\subset$ ” is obvious. To prove the inclusion “ $\supset$ ” it suffices to show that

$$\psi_j: k[G[j]/N[j]] \otimes_k {}^\sigma(k[G[j]/N[j])) \longrightarrow k[G[j+1]/N[j+1]], \quad f_1 \otimes (\lambda \otimes f_2) \mapsto f_1 \lambda \sigma(f_2)$$

is surjective for  $j \geq m$ . With  $\pi_{j+1}$  and  $\sigma_{j+1}$  as in (4) the morphisms

$$G[j+1] \xrightarrow{\pi_{j+1}} G[j] \rightarrow G[j]/N[j] \text{ and } G[j+1] \xrightarrow{\sigma_{j+1}} {}^\sigma(G[j]) \rightarrow {}^\sigma(G[j]/N[j])$$

combine to a morphism

$$G[j+1] \rightarrow (G[j]/N[j]) \times {}^\sigma(G[j]/N[j])$$

of algebraic groups with kernel  $(N[j] \times {}^{\sigma^j}\mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(N[j])) = N[j+1]$ . Therefore

$$G[j+1]/N[j+1] \longrightarrow (G[j]/N[j]) \times {}^\sigma(G[j]/N[j])$$

is a closed embedding and so the dual map is surjective, but the dual map is precisely  $\psi_j$ . We have thus proved (13). It follows from (13) that  $k\{G[m]/N[m]\} \rightarrow k\{G/N\}$  is surjective, i.e.,  $G/N$  is a  $\sigma$ -closed subgroup of  $G[m]/N[m]$ . As the ring to the left hand side of (13) is the coordinate ring of the  $i$ -th order Zariski closure of  $G/N$  in  $G[m]/N[m]$ , we obtain the required equality of the Zariski closures.  $\square$

The following example shows that in general one can not take  $m = 0$  in Proposition 7.7.

**Example 7.8.** Let  $G = \mathcal{G} = \mathbb{G}_a$  and  $N \trianglelefteq G$  the  $\sigma$ -closed subgroup given by  $N(R) = \{g \in R \mid \sigma(g) = 0\}$  for any  $k$ - $\sigma$ -algebra  $R$ . Then  $N[0] = G[0] = \mathbb{G}_a$  and  $G[0]/N[0]$  is the trivial group. Therefore  $G/N$  can not be a  $\sigma$ -closed subgroup of  $G[0]/N[0]$ .

**Corollary 7.9.** Let  $G$  be a  $\sigma$ -algebraic group and  $N \trianglelefteq G$  a normal  $\sigma$ -closed subgroup. Then

$$\sigma\text{-dim}(G) = \sigma\text{-dim}(N) + \sigma\text{-dim}(G/N) \quad (14)$$

and

$$\text{ord}(G) = \text{ord}(N) + \text{ord}(G/N). \quad (15)$$

*Proof.* We may assume that  $G$  is a  $\sigma$ -closed subgroup of some algebraic group  $\mathcal{G}$  (Theorem 2.13). For  $i \geq 0$  let  $G[i]$  and  $N[i]$  denote the  $i$ -th order Zariski closure of  $G$  and  $N$  in  $\mathcal{G}$  respectively. By Theorem 3.5 there exist  $e_G, e_N \geq 0$  such that  $\dim(G[i]) = \sigma\text{-dim}(G)(i+1) + e_G$  and  $\dim(N[i]) = \sigma\text{-dim}(N)(i+1) + e_N$  for  $i \gg 0$ . Let  $m \geq 0$  be as in Proposition 7.7 and for  $i \geq 0$  let  $(G/N)[i]$  denote the  $i$ -th order Zariski closure of  $G/N$  in  $G[m]/N[m]$ . By Theorem 3.5 there exist  $e_{G/N} \geq 0$  such that  $\dim((G/N)[i]) = \sigma\text{-dim}(G/N)(i+1) + e_{G/N}$ . For  $i \gg 0$

$$\begin{aligned} \sigma\text{-dim}(G/N)(i+1) + e_{G/N} &= \dim((G/N)[i]) = \dim(G[m+i]/N[m+i]) = \\ &= \dim(G[m+i]) - \dim(N[m+i]) = \\ &= \sigma\text{-dim}(G)(m+i+1) + e_G - \sigma\text{-dim}(N)(m+i+1) - e_N = \\ &= (\sigma\text{-dim}(G) - \sigma\text{-dim}(N))(i+1) + (\sigma\text{-dim}(G) - \sigma\text{-dim}(N))m + e_G - e_N. \end{aligned}$$

This proves (14). As  $\text{ord}(G) < \infty$  if and only if  $\sigma\text{-dim}(G) = 0$ , it follows from (14) that (15) is valid if  $\sigma\text{-dim}(G) > 0$ . We can therefore assume that  $\sigma\text{-dim}(G) = 0$ , and consequently  $\sigma\text{-dim}(N) = \sigma\text{-dim}(G/N) = 0$  as well. But then  $\text{ord}(G/N) = e_{G/N} = e_G - e_N = \text{ord}(G) - \text{ord}(N)$ .  $\square$

Next we will show how to compute  $\text{ld}(G/N)$  from  $\text{ld}(N)$  and  $\text{ld}(G)$ . For clarity of the exposition, we single out a simple lemma on algebraic groups.

**Lemma 7.10.** Let  $N_1 \trianglelefteq G_1$  and  $N_2 \trianglelefteq G_2$  be algebraic groups and  $\phi: G_2 \rightarrow G_1$  a surjective morphism of algebraic groups with kernel  $\mathcal{G}$ . Assume that the restriction of  $\phi$  to  $N_2$  has kernel  $\mathcal{N}$  and maps  $N_2$  surjectively onto  $N_1$ . Then the kernel of the induced map  $G_2/N_2 \rightarrow G_1/N_1$  is isomorphic to  $\mathcal{G}/\mathcal{N}$ .

*Proof.* Since  $\phi$  is surjective we may identify  $G_1$  with  $G_2/\mathcal{G}$ . Note that the (Noether) isomorphism theorems also hold for algebraic groups. (See e.g., [Mil12, Chapter IX]). We have  $N_1 = N_2/\mathcal{N} = N_2/\mathcal{G} \cap \mathcal{N}_2 = N_2\mathcal{G}/\mathcal{G}$  and so  $G_1/N_1 = (G_2/\mathcal{G})/(N_2\mathcal{G}/\mathcal{G}) = G_2/N_2\mathcal{G}$ . This shows that the kernel of  $G_2/N_2 \rightarrow G_1/N_1 = G_2/N_2\mathcal{G}$  equals  $N_2\mathcal{G}/N_2 = \mathcal{G}/N_2 \cap \mathcal{G} = \mathcal{G}/\mathcal{N}$ .  $\square$



**Corollary 7.11.** *Let  $G$  be a  $\sigma$ -algebraic group and  $N \trianglelefteq G$  a normal  $\sigma$ -closed subgroup. Then*

$$\text{ld}(G) = \text{ld}(G/N) \cdot \text{ld}(N).$$

*Proof.* By Remark 6.3 and Corollary 7.9 the claim is valid if  $\sigma\text{-dim}(G) > 0$ . So we may assume that  $\sigma\text{-dim}(G) = 0$  and therefore  $\text{ld}(G)$ ,  $\text{ld}(G/N)$  and  $\text{ld}(N)$  are all finite. Let  $m \geq 0$  be as in Proposition 7.7. For  $i \geq 1$  we have commutative diagrams

$$\begin{array}{ccc} (G/N)[i] & \xrightarrow{\pi_i} & (G/N)[i-1] \\ \downarrow \simeq & & \downarrow \simeq \\ G[m+i]/N[m+i] & \xrightarrow{\phi_i} & G[m+i-1]/N[m+i-1] \end{array}$$

where  $\phi_i$  is induced from the projection  $G[m+i] \twoheadrightarrow G[m+i-1]$ . For  $i \gg 0$  we have  $\text{ld}(G/N) = |\ker(\pi_i)| = |\ker(\phi_i)|$ . Let  $\mathcal{G}_{m+i}$  and  $\mathcal{N}_{m+i}$  be the kernel of  $G[m+i] \twoheadrightarrow G[m+i-1]$  and  $N[m+i] \twoheadrightarrow N[m+i-1]$  respectively. It follows from Lemma 7.10 that  $\ker(\phi_i) = \mathcal{G}_{m+i}/\mathcal{N}_{m+i}$ . Therefore

$$\text{ld}(G/N) = |\mathcal{G}_{m+i}/\mathcal{N}_{m+i}| = |\mathcal{G}_{m+i}|/|\mathcal{N}_{m+i}| = \text{ld}(G)/\text{ld}(N).$$

□

## 8 Morphisms

In this section we characterize the analogs of injective and surjective morphisms in the category of groups. Analogous results for algebraic groups are in [Mil12, Chapter VII].

**Theorem 8.1.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups. Then the following statements are equivalent:*

- (i) *The kernel of  $\phi$  is trivial.*
- (ii) *The map  $\phi_R: G(R) \rightarrow H(R)$  is injective for every  $k$ - $\sigma$ -algebra  $R$ .*
- (iii) *The morphism  $\phi: G \rightarrow H$  is a  $\sigma$ -closed embedding.*
- (iv) *The dual map  $\phi^*: k\{H\} \rightarrow k\{G\}$  is surjective.*
- (v) *The morphism  $\phi: G \rightarrow H$  is a monomorphism in the category of  $\sigma$ -algebraic groups, i.e., for every pair  $\phi_1, \phi_2: H' \rightarrow G$  of morphisms of  $\sigma$ -algebraic groups with  $\phi\phi_1 = \phi\phi_2$  we have  $\phi_1 = \phi_2$ .*

*Proof.* Clearly (i)  $\Leftrightarrow$  (ii), (iii)  $\Rightarrow$  (ii) and (ii)  $\Rightarrow$  (v). Moreover, (iii) and (iv) are equivalent by Lemma 1.6. So it suffices to show that (v) implies (iv). Define  $H' = G \times_H G$  by

$$(G \times_H G)(R) = \{(g_1, g_2) \in G(R) \times G(R) \mid \phi(g_1) = \phi(g_2)\}$$

for any  $k$ - $\sigma$ -algebra  $R$ . This is a  $\sigma$ -closed subgroup of  $G \times G$ . Indeed,  $G \times_H G$  is represented by  $k\{G\} \otimes_{k\{H\}} k\{G\}$ . Let  $\phi_1$  and  $\phi_2$  denote the projections onto the first and second coordinate respectively. We have  $\phi\phi_1 = \phi\phi_2$  and so by (v) we must have  $\phi_1 = \phi_2$ . This implies that the maps  $f \mapsto f \otimes 1$  and  $f \mapsto 1 \otimes f$  from  $k\{G\} \rightarrow k\{G\} \otimes_{k\{H\}} k\{G\}$  are equal. As  $\phi^*(k\{H\})$  is a Hopf subalgebra of  $k\{G\}$  we know that  $k\{G\}$  is faithfully flat over  $\phi^*(k\{H\})$  ([Wat79, Chapter 14]). Therefore  $f \otimes 1 = 1 \otimes f$  in  $k\{G\} \otimes_{k\{H\}} k\{G\} = k\{G\} \otimes_{\phi^*(k\{H\})} k\{G\}$  if and only if  $f \in \phi^*(k\{H\})$  by [Wat79, Section 13.1, p. 104]. Summarily, we find that  $\phi^*: k\{H\} \rightarrow k\{G\}$  is surjective. □

**Definition 8.2.** *A morphism of  $\sigma$ -algebraic groups satisfying the equivalent properties of Theorem 8.1 is called injective.*

**Example 8.3.** The morphism  $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m$  given by  $\phi_R(g) = \sigma(g)$  for any  $k$ - $\sigma$ -algebra  $R$  and  $g \in R^\times$  is not injective. Even though  $\phi_R$  is injective for every  $\sigma$ -field extension  $R$  of  $k$ .

Recall that in Lemma 1.5 we defined  $\phi(X)$  for a morphism  $\phi: X \rightarrow Y$  of  $\sigma$ -varieties.

**Lemma 8.4.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups and  $G_1$  a  $\sigma$ -closed subgroup of  $G$ . Then  $\phi(G_1)$  is a  $\sigma$ -closed subgroup of  $H$ .*

*Proof.* We may assume that  $G_1 = G$ . It follows from the proof of Lemma 1.5 that  $\phi(G) = \mathbb{V}(\mathfrak{a})$ , where  $\mathfrak{a}$  is the kernel of  $\phi^*: k\{H\} \rightarrow k\{G\}$ . Since  $\phi^*$  is a morphism of  $k$ - $\sigma$ -Hopf algebras,  $\mathfrak{a}$  is a  $\sigma$ -Hopf ideal. So  $\phi(G)$  is a  $\sigma$ -closed subgroup of  $H$ .  $\square$

**Theorem 8.5.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups. The following statements are equivalent:*

- (i)  $\phi(G) = H$ .
- (ii) *The morphism  $\phi$  is a quotient, i.e., there exists a normal  $\sigma$ -closed subgroup  $N$  of  $G$  such  $\phi$  is the quotient of  $G$  mod  $N$ .*
- (iii) *The dual map  $\phi^*: k\{H\} \rightarrow k\{G\}$  is injective.*
- (iv) *For every  $k$ - $\sigma$ -algebra  $R$  and every  $h \in H(R)$ , there exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $g \in G(S)$  such that the image of  $h$  in  $H(S)$  equals  $\phi(g)$ .*

*Proof.* We know from Lemma 1.5 that  $\phi(G)$  is the  $\sigma$ -closed  $\sigma$ -subvariety of  $H$  defined by  $\ker(\phi^*)$ . Therefore (i) and (iii) are equivalent. It is clear from Theorem 7.3 that (iii) and (ii) are equivalent. Moreover (ii) implies (iv) by Lemma 7.5. It thus suffices to show that (iv) implies (iii). Take  $R = k\{H\}$  and  $h = \text{id}_{k\{H\}} \in H(R) = \text{Hom}(k\{H\}, k\{H\})$ . By (iv) there exists a faithfully flat morphism  $\psi: k\{H\} \rightarrow S$  of  $k$ - $\sigma$ -algebras and an element  $g \in G(S) = \text{Hom}(k\{G\}, S)$  such that the image of  $h$  in  $H(S) = \text{Hom}(k\{H\}, S)$  equals  $\phi(g) = g\phi^*$ . This means that  $\psi = g\phi^*$ . As any faithfully flat morphism of rings is injective,  $\psi$  is injective. Therefore  $\phi^*$  is injective as well.  $\square$

**Definition 8.6.** *A morphism of  $\sigma$ -algebraic groups satisfying the equivalent properties of Theorem 8.5 is called surjective.*

We write  $\phi: G \twoheadrightarrow H$  to express that  $\phi$  is surjective.

**Example 8.7.** The morphism  $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m$  given by  $\phi_R(g) = \sigma(g)$  for any  $k$ - $\sigma$ -algebra  $R$  and  $g \in R^\times$  is surjective since the dual map  $\phi^*: k\{y, y^{-1}\} \rightarrow k\{y, y^{-1}\}$ ,  $y \mapsto \sigma(y)$  is injective. Note that  $\phi_R$  need not be surjective.

**Corollary 8.8.** *A morphism of  $\sigma$ -algebraic groups which is injective and surjective is an isomorphism.*

*Proof.* By Theorems 8.1 and 8.5, an injective and surjective morphism of  $\sigma$ -algebraic groups induces a surjective and injective morphism on the  $\sigma$ -coordinate rings.  $\square$

**Corollary 8.9.** *Every morphism of  $\sigma$ -algebraic groups factors uniquely as a surjective morphism followed by an injective morphism.*

*Proof.* Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups. The uniqueness means that if  $G \twoheadrightarrow H_1 \hookrightarrow H$  and  $G \twoheadrightarrow H_2 \hookrightarrow H$  are two factorizations of  $\phi$ , then there exists an isomorphism  $H_1 \rightarrow H_2$  of  $\sigma$ -algebraic groups making

$$\begin{array}{ccccc} G & \twoheadrightarrow & H_1 & \hookrightarrow & H \\ \parallel & & \downarrow \simeq & & \parallel \\ G & \twoheadrightarrow & H_2 & \hookrightarrow & H \end{array}$$

commutative. By Theorem 4.5 the  $k$ - $\sigma$ -Hopf subalgebra  $\phi^*(k\{H\})$  of  $k\{G\}$  is finitely  $\sigma$ -generated over  $k$ . So we can define  $H_1$  as the  $\sigma$ -algebraic group represented by  $\phi^*(k\{H\})$ . The claim of the corollary follows immediately by dualizing.  $\square$

Note that  $H_1$  has two interpretations, either as  $\phi(G)$  or as  $G/\ker(\phi)$ . See Theorem 11.13.

As we will see in the sequel, point (iv) of Theorem 8.5 is very helpful to reduce certain questions to computations with group elements. Let  $X$  be a  $\sigma$ -variety. If  $R \rightarrow S$  is an injective morphism of  $k$ - $\sigma$ -algebras (e.g.,  $S$  is a faithfully flat  $R$ - $\sigma$ -algebra), then

$$X(R) = \text{Hom}(k\{X\}, R) \rightarrow \text{Hom}(k\{X\}, S) = X(S)$$

is injective. To simplify the notation, we will, in the sequel, often identify  $X(R)$  with its image in  $X(S)$ .

**Lemma 8.10.** *Let  $Y$  be a  $\sigma$ -closed  $\sigma$ -subvariety of a  $\sigma$ -variety  $X$  and  $R \rightarrow S$  an injective morphism of  $k$ - $\sigma$ -algebras (e.g.,  $R \rightarrow S$  is faithfully flat). Then*

$$Y(R) = X(R) \cap Y(S),$$

where, using the above described identification, the intersection is understood to take place in  $X(S)$ .

*Proof.* The inclusion “ $\subset$ ” is obvious. To prove “ $\supset$ ” it suffices to note that for a morphism  $k\{X\} \rightarrow S$  with factorizations  $k\{X\} \rightarrow k\{Y\} \rightarrow S$  and  $k\{X\} \rightarrow R \hookrightarrow S$ , one has an arrow  $k\{Y\} \rightarrow R$  such that

$$\begin{array}{ccc} & k\{Y\} & \\ \nearrow & \vdots & \searrow \\ k\{X\} & & S \\ \searrow & \downarrow & \nearrow \\ & R & \end{array}$$

commutes. □

**Lemma 8.11.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups and  $G_1 \leq G$  a  $\sigma$ -closed subgroup. Let  $R$  be a  $k$ - $\sigma$ -algebra. Then  $\phi(G_1)(R)$  equals the set of all  $h \in H(R)$  such that there exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $g_1 \in G_1(S)$  with  $\phi(g_1) = h$ .*

*Proof.* The induced morphism  $G_1 \rightarrow \phi(G_1)$  is surjective. So it follows from Theorem 8.5 (iv) that for  $h \in \phi(G_1)(R)$  there exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $g_1 \in G_1(S)$  with  $\phi(g_1) = h$ .

Conversely, if  $h = \phi(g_1)$ , then  $h \in \phi(G_1(S)) \subset \phi(G_1)(S)$  and it follows from  $\phi(G_1)(S) \cap H(R) = \phi(G_1)(R)$  (Lemma 8.10) that  $h \in \phi(G_1)(R)$ . □

**Lemma 8.12.** *Let  $\phi: G \rightarrow H$  be a surjective morphism of  $\sigma$ -algebraic groups. If  $N$  is a normal  $\sigma$ -closed subgroup of  $G$ , then  $\phi(N)$  is a normal  $\sigma$ -closed subgroup of  $H$ .*

*Proof.* Let  $R$  be a  $k$ - $\sigma$ -algebra,  $h \in \phi(N)(R)$  and  $h_1 \in H(R)$ . We have to show that  $h_1 h h_1^{-1} \in \phi(N)(R)$ . By Theorem 8.5, there exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $g \in N(S)$  with  $\phi(g) = h$ . Similarly, there exists a faithfully flat  $R$ - $\sigma$ -algebra  $S_1$  and  $g_1 \in G(S_1)$  with  $\phi(g_1) = h_1$ . Then  $S' = S \otimes_R S_1$  is a faithfully flat  $R$ - $\sigma$ -algebra ([Wat79, Section 13.3, p. 106]) and we can consider  $G(S)$  and  $G(S_1)$  as subgroups of  $G(S')$ . Since  $N(S') \trianglelefteq G(S')$  we see that  $g_1 g g_1^{-1} \in N(S')$ . Therefore  $\phi(g_1 g g_1^{-1}) = h_1 h h_1^{-1} \in \phi(N(S')) \subset \phi(N)(S')$ . As  $\phi(N)(S') \cap H(R) = \phi(N)(R)$  by Lemma 8.10, this shows that  $h_1 h h_1^{-1} \in \phi(N)(R)$ . □

## 9 Components

In [Hru04, Section 4.6] E. Hrushovski raised the question whether or not it is possible to strengthen the classical Ritt–Raudenbusch basis theorem ([Lev08, Theorem 2.5.11]). For clarity, let us state the question as a conjecture:

**Conjecture 1.** *Let  $k$  be a  $\sigma$ -field and  $R$  a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra. Then every ascending chain of radical, mixed  $\sigma$ -ideals in  $R$  is finite.*

Here a  $\sigma$ -ideal  $\mathfrak{a}$  is called mixed, if  $ab \in \mathfrak{a}$  implies  $a\sigma(b) \in \mathfrak{a}$ . E. Hrushovski proved Conjecture 1 under certain additional assumptions on  $R$ . (See [Hru04, Lemma 4.35].) In [Lev] A. Levin showed that the conjecture fails if the assumption that the  $\sigma$ -ideals are radical is dropped.

A prime  $\sigma$ -ideal  $\mathfrak{p}$  of a  $\sigma$ -ring  $R$  is called minimal if for every prime  $\sigma$ -ideal  $\mathfrak{q}$  of  $R$  with  $\mathfrak{q} \subset \mathfrak{p}$  we have  $\mathfrak{q} = \mathfrak{p}$ . Using [Hru04, Lemma 4.34] one can show that Conjecture 1 is equivalent to the following:

**Conjecture 2.** *Let  $k$  be a  $\sigma$ -field and  $R$  a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra. Then the set of minimal prime  $\sigma$ -ideals of  $R$  is finite.*

One of the main results of this section is a special case of the above conjecture:

**Theorem 9.1.** *Conjecture 2 holds under the additional assumption that  $R$  can be equipped with the structure of a  $k$ - $\sigma$ -Hopf algebra.*

The proof of Theorem 9.1 is given at the end of this section. More generally, in this section we study the components of a  $\sigma$ -algebraic group. The matter is complicated by the fact that, contrary to the case of algebraic groups or differential algebraic groups, a  $\sigma$ -algebraic group may have infinitely many components. However, as indicated in Theorem 9.1, a  $\sigma$ -algebraic group has only finitely many “ $\sigma$ -components”.

To be able to speak meaningfully of topological notions, such as connected components, we first need to clarify what is the topological space associated to a  $\sigma$ -algebraic group. By the underlying topological space of a  $\sigma$ -algebraic group  $G$  we mean the underlying topological space of the scheme  $G^\sharp$ . In other words, the underlying topological space of  $G$  is  $\text{Spec}(k\{G\})$ . The reader might wonder if not some difference analog of  $\text{Spec}(-)$  would provide a more adequate notion. For example (cf. [Hru04]), one could consider the space of all  $\sigma$ -prime  $\sigma$ -ideals of  $k\{G\}$  instead of the space of all prime ideals of  $k\{G\}$ . (Recall that a prime  $\sigma$ -ideal  $\mathfrak{p}$  is called  $\sigma$ -prime if  $\sigma^{-1}(\mathfrak{p}) = \mathfrak{p}$ .) However, there often are not “enough”  $\sigma$ -prime  $\sigma$ -ideals. In general, a  $\sigma$ -ring need not contain a  $\sigma$ -prime  $\sigma$ -ideal. This pathology does not occur for  $\sigma$ -algebraic groups, since the kernel  $\mathfrak{m}$  of the counit  $k\{G\} \rightarrow k$  is a  $\sigma$ -prime  $\sigma$ -ideal. But it may happen that  $\mathfrak{m}$  is the only  $\sigma$ -prime  $\sigma$ -ideal of  $k\{G\}$ , even if  $G$  is quite far from being the trivial group:

**Example 9.2.** For all  $\sigma$ -algebraic groups in the following list, the  $\sigma$ -ideal  $\mathfrak{m}$  is the only  $\sigma$ -prime  $\sigma$ -ideal of  $k\{G\}$ . (Equivalently,  $G(K) = 1$  for every  $\sigma$ -field extension  $K$  of  $k$ . Cf. Remark 10.3.)

- $G(R) = \{g \in \text{GL}_n(R) \mid \sigma(g_{ij}) = \delta_{ij}\} \leq \text{GL}_n(R)$
- $G(R) = \{g \in R \mid \sigma^n(g) = 0\} \leq \mathbb{G}_a(R)$  for some  $n \geq 1$ .
- $G(R) = \{g \in R \mid g^n = 1, \sigma(g) = 1\} \leq \mathbb{G}_m(R)$  for some  $n \geq 1$ .
- $G(R) = \{g \in R \mid g^3 = 1, \sigma(g) = g\} \leq \mathbb{G}_m(R)$ , where  $k$  contains two non-trivial third roots of unity which are permuted by  $\sigma: k \rightarrow k$ .
- $G(R) = \{g \in R^\times \mid g^p = 1\} \leq \mathbb{G}_m(R)$  where  $k$  has characteristic  $p > 0$ .
- $G(R) = \{g \in R^\times \mid g^p = 1, \sigma^2(g) = g^3\} \leq \mathbb{G}_m(R)$  where  $k$  has characteristic  $p > 0$ .
- Let  $\mathbf{G}$  be a finite group and  $\Sigma: \mathbf{G} \rightarrow \mathbf{G}$  a group endomorphism with only one fixed point (for example,  $\Sigma(g) = 1$  for  $g \in \mathbf{G}$ ). Let  $G$  be the corresponding  $\sigma$ -algebraic group constructed in Example 2.12.

As usual, by an *irreducible component* of a topological space we mean a maximal irreducible subset. By a *connected component* of a topological space we mean a maximal connected subset. An irreducible (or connected) component is automatically closed. Every topological space is the disjoint union of its connected components.

By a connected (or irreducible) component of a  $\sigma$ -algebraic group  $G$  we mean a connected (or irreducible) component of the underlying topological space of  $G$ . If  $R$  is a ring and  $\mathfrak{a} \subset R$ , let us denote by  $\mathcal{V}(\mathfrak{a})$  the closed subset of  $\text{Spec}(R)$  defined by  $\mathfrak{a}$ .

**Lemma 9.3.** *Let  $G$  be a  $\sigma$ -algebraic group. The connected components and the irreducible components of  $G$  coincide. Moreover, if  $\mathfrak{p}$  is a prime ideal of  $k\{G\}$ , then the connected component of  $G$  containing  $\mathfrak{p}$  equals  $\mathcal{V}(\mathfrak{a})$ , where  $\mathfrak{a}$  is the ideal of  $k\{G\}$  generated by all idempotent elements of  $k\{G\}$  contained in  $\mathfrak{p}$ .*

*Proof.* Let us fix a  $\sigma$ -closed embedding  $G \hookrightarrow \mathcal{G}$  of  $G$  into some algebraic group  $\mathcal{G}$  and for  $i \geq 0$  let  $G[i]$  denote the  $i$ -th order Zariski-closure of  $G$  in  $\mathcal{G}$ . Let  $C \subset \text{Spec}(k\{G\})$  denote a connected component of  $G$ . Then  $C = \mathcal{V}(\mathfrak{a})$  for a unique ideal  $\mathfrak{a}$  of  $k\{G\}$  generated by idempotent elements. (See [Sta14, Tag 00EB].) For every  $i \geq 0$ , the closure of the image of  $C$  under the projection  $G^\sharp \rightarrow G[i]$  is connected and equal to  $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset G[i]$ . So  $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset G[i]$  is contained in a connected component of  $G[i]$ . Assume that  $G[i]$  has  $n_i$  connected components. Then

$$k[G[i]] = e_{i,1}k[G[i]] \oplus \cdots \oplus e_{i,n_i}k[G[i]]$$

for some primitive idempotent elements  $e_{i,1}, \dots, e_{i,n_i} \in k[G[i]]$  and  $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset \mathcal{V}(\mathfrak{b}_i)$  where  $\mathfrak{b}_i = (e_{i,1}, \dots, e_{i,j_i-1}, e_{i,j_i+1}, \dots, e_{i,n_i}) \subset k[G[i]]$  for a unique  $j_i \in \{1, \dots, n_i\}$ . We have  $\mathfrak{b}_{i+1} \cap k[G[i]] = \mathfrak{b}_i$  for  $i \geq 0$  and  $\mathfrak{b} := \bigcup_{i \geq 0} \mathfrak{b}_i$  is an ideal of  $k\{G\}$ . From  $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset \mathcal{V}(\mathfrak{b}_i)$  it follows that  $\mathfrak{b}_i$  is contained in the radical of  $\mathfrak{a} \cap k[G[i]]$ . Since the  $e_{i,j}$ ’s are idempotent this shows that  $\mathfrak{b}_i \subset \mathfrak{a}$ . So  $\mathfrak{b} \subset \mathfrak{a}$ .

Since  $k\{G\}/\mathfrak{b}$  may be interpreted as the directed union of the algebras  $k[G[i]]/\mathfrak{b}_i \simeq e_{i,j_i} k[G[i]]$  which have a prime nilradical, it is clear that  $\mathcal{V}(\mathfrak{b})$  is irreducible (and a fortiori connected). As  $C = \mathcal{V}(\mathfrak{a}) \subset \mathcal{V}(\mathfrak{b})$  it follows from the maximality of  $C$  that  $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{b})$ . By the uniqueness of  $\mathfrak{a}$  we have  $\mathfrak{a} = \mathfrak{b}$ .

We have thus shown that every connected component of  $G$  is irreducible. So the connected and the irreducible components of  $G$  coincide.

The claimed form of the connected component of a prime ideal of  $k\{G\}$  follows from the above arguments.  $\square$

Since the connected components and the irreducible components of a  $\sigma$ -algebraic group coincide, we will speak simply of the *components of a  $\sigma$ -algebraic group* in the sequel. The components of a  $\sigma$ -algebraic group  $G$  are in bijection with the minimal prime ideals of  $k\{G\}$ . The following simple example shows that a  $\sigma$ -algebraic group can have infinitely many components and that the components need not be open.

**Example 9.4.** Let  $G \leq \mathbb{G}_m$  be the  $\sigma$ -algebraic group given by

$$G(R) = \{g \in R^\times \mid g^2 = 1\} \leq \mathbb{G}_m(R)$$

for any  $k$ - $\sigma$ -algebra  $R$ . We have

$$k\{G\} = k[y]/[y^2 - 1] = k[y, \sigma(y), \dots]/(y^2 - 1, \sigma(y)^2 - 1, \dots).$$

Let us assume that the characteristic of  $k$  is not equal to 2. Then the prime ideals of  $k\{G\}$  are in bijection with the set of all sequences  $(a_i)_{i \in \mathbb{N}}$  such that  $a_i \in \{1, -1\}$ . Every prime ideal of  $k\{G\}$  is its own component. In particular,  $G$  has infinitely many components. The open subsets of  $\text{Spec}(k\{G\})$  are all infinite, thus the components are not open.

Allowing ourselves a little abuse of notation we denote the canonical map

$$\text{Spec}(k\{G\}) \rightarrow \text{Spec}(k\{G\}), \mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p})$$

also by  $\sigma$ .

**Definition 9.5.** A component  $C$  of a  $\sigma$ -algebraic group is called a  $\sigma$ -component if  $\sigma(C) \subset C$ .

**Example 9.6.** The  $\sigma$ -algebraic group from Example 9.4 has two  $\sigma$ -components, namely the prime ideals corresponding to the sequences  $(1, 1, \dots)$  and  $(-1, -1, \dots)$ .

**Lemma 9.7.** Let  $G$  be a  $\sigma$ -algebraic group and  $C \subset \text{Spec}(k\{G\})$  a component of  $G$ . Let  $\mathfrak{p} \subset k\{G\}$  be the prime ideal and  $\mathfrak{a} \subset k\{G\}$  the ideal generated by idempotent elements such that  $C = \mathcal{V}(\mathfrak{p}) = \mathcal{V}(\mathfrak{a})$ . Then the following conditions are equivalent:

- (i) The component  $C$  is a  $\sigma$ -component.
- (ii) The ideal  $\mathfrak{a}$  is a  $\sigma$ -ideal.
- (iii) The ideal  $\mathfrak{p}$  is a  $\sigma$ -ideal.
- (iv) There exists a prime  $\sigma$ -ideal in  $C$ .
- (v) There exists a  $\sigma$ -prime  $\sigma$ -ideal in  $C$ .
- (vi) The set of all idempotent elements contained in  $\mathfrak{a}$  is stable under  $\sigma$ .

*Proof.* The equivalence of (i) and (iii) is straightforward. As  $\mathfrak{p}$  is the radical of  $\mathfrak{a}$  we see that (ii) implies (iii). Clearly (iii) implies (iv). If  $\mathfrak{q}$  is a  $\sigma$ -ideal in  $C$ , then its reflexive closure  $\mathfrak{q}^* = \{f \in k\{G\} \mid \exists n \geq 0 : \sigma^n(f) \in \mathfrak{q}\}$  is a  $\sigma$ -prime  $\sigma$ -ideal in  $C$  (cf. [Lev08, p. 107] and Section 10 below). So (iv) implies (v).

Let us next show that (v) implies (vi). If  $\mathfrak{q}$  is a  $\sigma$ -prime  $\sigma$ -ideal in  $C$ , then by Lemma 9.3 we have  $C = \mathcal{V}(\mathfrak{a}')$  where  $\mathfrak{a}' \subset k\{G\}$  is the ideal generated by all idempotent elements contained in  $\mathfrak{q}$ . By [Sta14, Tag 00EB] we must have  $\mathfrak{a}' = \mathfrak{a}$ . Now let  $e \in \mathfrak{a}$  be an idempotent. We have to show that  $\sigma(e) \in \mathfrak{a}$ . But  $e \in \mathfrak{q}$  (as  $\mathfrak{q} \in C = \mathcal{V}(\mathfrak{a})$ ) and consequently  $\sigma(e) \in \mathfrak{q}$  is also idempotent. So  $\sigma(e) \in \mathfrak{a}' = \mathfrak{a}$ .

Finally, the implication (vi)  $\Rightarrow$  (ii) follows from the simple fact that an ideal generated by a  $\sigma$ -stable set is a  $\sigma$ -ideal.  $\square$

**Corollary 9.8.** *Let  $k\{G\}$  be a  $k$ - $\sigma$ -Hopf algebra which is finitely  $\sigma$ -generated over  $k$ . Then a minimal prime  $\sigma$ -ideal of  $k\{G\}$  is a minimal prime ideal of  $k\{G\}$ .*

*Proof.* Let  $\mathfrak{q} \subset k\{G\}$  be a minimal prime  $\sigma$ -ideal and let  $C \subset \text{Spec}(k\{G\})$  be the component which contains  $\mathfrak{q}$ . Then  $C = \mathcal{V}(\mathfrak{p})$  for a minimal prime ideal  $\mathfrak{p}$  of  $k\{G\}$ . Since  $\mathfrak{q} \in C$  it follows from Lemma 9.7 that  $\mathfrak{p}$  is a  $\sigma$ -ideal. Therefore  $\mathfrak{q} = \mathfrak{p}$  by the minimality of  $\mathfrak{q}$ .  $\square$

We will next introduce  $\sigma$ -étale  $\sigma$ -algebraic groups. The role of these groups in the theory of  $\sigma$ -algebraic groups is in a certain sense analogous to the role of étale algebraic groups in the theory of algebraic groups. We plan to study  $\sigma$ -étale  $\sigma$ -algebraic groups in more detail in a future paper. In particular, these groups are expected to satisfy a certain decomposition theorem. Here we will only use them to define the group of components and the identity component of a  $\sigma$ -algebraic group.

**Definition 9.9.** *A finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra  $R$  is called  $\sigma$ -étale (over  $k$ ) if  $R$  is integral over  $k$  and a separable  $k$ -algebra.*

Thus a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra  $R$  is  $\sigma$ -étale if and only if for every  $r \in R$  there exists a separable polynomial  $f$  over  $k$  with  $f(r) = 0$ . Similar notions of étaleness in difference algebra occur in [Tom14] and [Tom] in a slightly different setting.

**Definition 9.10.** *A  $\sigma$ -algebraic group  $G$  is called  $\sigma$ -étale if  $k\{G\}$  is  $\sigma$ -étale over  $k$ .*

**Theorem 9.11.** *Let  $G$  be a  $\sigma$ -algebraic group. There exists a  $\sigma$ -étale  $\sigma$ -algebraic group  $\pi_0(G)$  and a morphism  $G \rightarrow \pi_0(G)$  of  $\sigma$ -algebraic groups satisfying the following universal property: If  $G \rightarrow H$  is a morphism of  $\sigma$ -algebraic groups with  $H$   $\sigma$ -étale, then there exists a unique morphism  $\pi_0(G) \rightarrow H$  such that*

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \pi_0(G) \\ & \searrow & \swarrow \text{dotted} \\ & H & \end{array}$$

*commutes.*

*Proof.* Let  $R \subset k\{G\}$  denote the set of all elements  $r \in k\{G\}$  which annul a separable polynomial over  $k$ . (So  $R$  is the union of all étale subalgebras of  $k\{G\}$ .) Then  $R$  is a  $k$ -subalgebra of  $k\{G\}$ . Indeed,  $R$  is a Hopf subalgebra of  $k\{G\}$ . (Cf. Section 6.7 in [Wat79].)

Let  $r \in R$  and  $f$  be a separable polynomial over  $k$  with  $f(r) = 0$ . Let  ${}^\sigma f$  denote the polynomial obtained from  $f$  by applying  $\sigma$  to the coefficients. Then  ${}^\sigma f$  is separable and  ${}^\sigma f(\sigma(r)) = 0$ . This shows that  $R$  is a  $k$ - $\sigma$ -Hopf subalgebra of  $k\{G\}$ . Let  $\pi_0(G)$  denote the  $\sigma$ -étale  $\sigma$ -algebraic group corresponding to  $R$  and  $G \rightarrow \pi_0(G)$  the morphism corresponding to the inclusion  $R \subset k\{G\}$ .

If  $G \rightarrow H$  is a morphism of  $\sigma$ -algebraic groups with  $H$   $\sigma$ -étale, then the image of the dual map  $k\{H\} \rightarrow k\{G\}$  consists of elements that annul a separable polynomial. Thus the image lies in  $R$  and  $k\{H\} \rightarrow k\{G\}$  factors uniquely through  $R \hookrightarrow k\{G\}$ .  $\square$

Of course  $\pi_0(G)$  is unique up to unique isomorphisms. It is clear from the above proof that  $G \rightarrow \pi_0(G)$  is surjective.

**Definition 9.12.** *Let  $G$  be a  $\sigma$ -algebraic group. The  $\sigma$ -étale  $\sigma$ -algebraic group  $\pi_0(G)$  defined by the universal property from Theorem 9.11 is called the group of components of  $G$ . The kernel  $G^\circ$  of  $G \rightarrow \pi_0(G)$  is called the identity component of  $G$ .*

So  $G/G^\circ = \pi_0(G)$ .

**Lemma 9.13.** *Let  $G$  be a  $\sigma$ -algebraic group. There is a one-to-one correspondence between the components of  $G$  and the components of  $\pi_0(G)$ . Under this bijection  $\sigma$ -components correspond to  $\sigma$ -components. Moreover, every component of  $\pi_0(G)$  consists of a single point.*

*Proof.* Every prime ideal of  $k\{\pi_0(G)\}$  is maximal and hence also minimal. This shows that the components of  $\pi_0(G)$  are points. We identify  $k\{\pi_0(G)\}$  with its image in  $k\{G\}$ . We claim that  $\mathfrak{p} \mapsto \mathfrak{p} \cap k\{\pi_0(G)\}$  is a bijection between the minimal prime ideals of  $k\{G\}$  and the (minimal) prime ideals of  $k\{G\}$ . Every (minimal) prime ideal of  $k\{\pi_0(G)\}$  is of the form  $\mathfrak{p} \cap k\{\pi_0(G)\}$  for some minimal prime ideal of  $k\{G\}$  ([Bou72, Proposition 16, Chapter II, §2.6]). On the other hand, if  $\mathfrak{p}$  is a minimal prime ideal of  $k\{G\}$ ,

then  $\mathfrak{p} = \sqrt{\mathfrak{a}}$  for some ideal  $\mathfrak{a}$  of  $k\{G\}$  generated by idempotent elements. Since all idempotent elements of  $k\{G\}$  lie in  $k\{\pi_0(G)\}$ , we see that  $(\mathfrak{a} \cap k\{\pi_0(G)\}) = \mathfrak{a}$ . Therefore  $\sqrt{(\mathfrak{p} \cap k\{\pi_0(G)\})} = \mathfrak{p}$ .

If  $\mathfrak{p}$  is a  $\sigma$ -ideal, then  $\mathfrak{p} \cap k\{\pi_0(G)\}$  is a  $\sigma$ -ideal. Conversely, if  $\mathfrak{p}' \subset k\{\pi_0(G)\}$  is a  $\sigma$ -ideal, then  $\sqrt{(\mathfrak{p}')} \subset k\{G\}$  is a  $\sigma$ -ideal.  $\square$

**Proposition 9.14.** *The following four conditions on a  $\sigma$ -algebraic group  $G$  are equivalent:*

- (i)  $G^\circ = G$ .
- (ii)  $\pi_0(G) = 1$ .
- (iii) *The topological space of  $G$  is connected.*
- (iv) *The nilradical of  $k\{G\}$  is a prime ideal.*

*Proof.* Clearly, (i)  $\Leftrightarrow$  (ii). We have (ii)  $\Leftrightarrow$  (iii) by Lemma 9.13. Since the connected components are irreducible (Lemma 9.3), it follows from (iii) that  $k\{G\}$  has a unique minimal prime ideal, which must then equal the nilradical. Thus (iii)  $\Rightarrow$  (iv). On the other hand (iv) means that the topological space of  $G$  is irreducible. So (iv)  $\Rightarrow$  (iii).  $\square$

**Definition 9.15.** *A  $\sigma$ -algebraic group satisfying the equivalent conditions of Proposition 9.14 is called connected.*

Note that the identity component  $G^\circ$  of a  $\sigma$ -algebraic group  $G$  is, strictly speaking, not a component. It carries more structure than a mere component, in particular it has the structure of a  $\sigma$ -variety. However, as illustrated in the proof of the following lemma, the topological space of  $G^\circ$  can be identified with the component of  $G$  which contains the identity  $\mathfrak{m}_{k\{G\}}$ , i.e., the kernel of the counit  $k\{G\} \rightarrow k$ .

**Lemma 9.16.** *Let  $G$  be a  $\sigma$ -algebraic group. Then  $G^\circ$  is connected.*

*Proof.* Every ideal of  $k\{\pi_0(G)\}$  is generated by idempotent elements. It follows that  $\mathfrak{m}_{k\{\pi_0(G)\}} = \mathfrak{m}_{k\{G\}} \cap k\{\pi_0(G)\}$  is generated by all idempotent elements contained in  $\mathfrak{m}_{k\{G\}}$ . Therefore,  $\mathbb{I}(G^\circ)$  is the ideal of  $k\{G\}$  generated by all idempotent elements of  $k\{G\}$  contained in  $\mathfrak{m}_{k\{G\}}$ . It follows from Lemma 9.3, that  $\mathcal{V}(\mathbb{I}(G^\circ)) \subset \text{Spec}(k\{G\})$  is connected. As  $\mathcal{V}(\mathbb{I}(G^\circ))$  and  $\text{Spec}(k\{G^\circ\}) = \text{Spec}(k\{G\}/\mathbb{I}(G^\circ))$  are homeomorphic, this implies that  $G^\circ$  is connected.  $\square$

**Lemma 9.17.** *Let  $G$  be a  $\sigma$ -closed subgroup of an algebraic group  $\mathcal{G}$  and for  $i \geq 0$  let  $G[i]$  and  $G^\circ[i]$  denote the  $i$ -th order Zariski closure of  $G$  and  $G^\circ$  in  $\mathcal{G}$  respectively. Then*

$$G^\circ[i] = G[i]^\circ.$$

*In particular,  $G$  is connected if and only if all its Zariski closures are connected.*

*Proof.* Both groups are defined by the ideal of  $k[G[i]] \subset k\{G\}$  which is generated by all idempotent elements of  $k[G[i]]$  contained in the kernel of the counit  $k[G[i]] \rightarrow k$ .  $\square$

**Corollary 9.18.** *Let  $G$  be a  $\sigma$ -algebraic group. Then  $\sigma\text{-dim}(G^\circ) = \sigma\text{-dim}(G)$  and  $\text{ord}(G^\circ) = \text{ord}(G)$ .*

*Proof.* Let  $\mathcal{G}$  be a  $\sigma$ -algebraic group containing  $G$  as a  $\sigma$ -closed subgroup. Then for  $i \geq 0$  we have  $\dim(G[i]) = \dim(G[i]^\circ) = \dim(G^\circ[i])$  by Lemma 9.17. Thus the claim follows from Theorem 3.5.  $\square$

The limit degree of  $G$  and  $G^\circ$  are in general distinct. Indeed  $\text{ld}(G) = \text{ld}(\pi_0(G))\text{ld}(G^\circ)$  by Corollary 7.11. We will next show that a  $\sigma$ -algebraic group has only finitely many  $\sigma$ -components.

**Lemma 9.19.** *Let  $R$  be a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra. If  $R$  is  $\sigma$ -étale, then  $R$  has only finitely many prime  $\sigma$ -ideals.*

*Proof.* Since  $R$  is  $\sigma$ -étale, every prime ideal of  $R$  is maximal and hence also minimal. If  $\mathfrak{p}$  is a prime  $\sigma$ -ideal of  $R$ , then  $\mathfrak{p} \subset \sigma^{-1}(\mathfrak{p})$  and therefore  $\mathfrak{p} = \sigma^{-1}(\mathfrak{p})$ . So every prime  $\sigma$ -ideal of  $R$  is  $\sigma$ -prime. It follows from the Ritt–Raudenbush basis theorem (cf. Theorems 2.5.11 and 2.5.7 in [Lev08]) that a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra has only finitely many minimal  $\sigma$ -prime ideals. Since every prime  $\sigma$ -ideal of  $R$  is a minimal  $\sigma$ -prime ideal of  $R$ , this implies that  $R$  has only finitely many prime  $\sigma$ -ideals.  $\square$

**Theorem 9.20.** *A  $\sigma$ -algebraic group has only finitely many  $\sigma$ -components.*

*Proof.* Let  $G$  be a  $\sigma$ -algebraic group. By Lemma 9.13, the  $\sigma$ -components of  $G$  are in bijection with the  $\sigma$ -components of  $\pi_0(G)$  and by Lemma 9.19 the  $\sigma$ -algebraic group  $\pi_0(G)$  has only finitely many  $\sigma$ -components.  $\square$

*Proof of Theorem 9.1.* By assumption  $R = k\{G\}$  for a  $\sigma$ -algebraic group  $G$ . By Corollary 9.8 the set of minimal prime  $\sigma$ -ideals of  $k\{G\}$  equals the set of minimal prime ideals of  $k\{G\}$  which are  $\sigma$ -ideals. The latter set is finite by Theorem 9.20.  $\square$

## 10 Subgroups defined by ideal closures

If  $\mathcal{G}$  is an algebraic group over a perfect field, then  $\mathcal{G}_{\text{red}}$ , the associated reduced scheme, is a closed subgroup of  $\mathcal{G}$ . In difference algebra, there are several closure operations one can define on difference ideals which are in some way similar to taking the radical of an ideal. Therefore we obtain several  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group which are in some way analogous to  $\mathcal{G}_{\text{red}}$ . Let us introduce now this closure operations on  $\sigma$ -ideals. (Cf. [Lev08, Section 2.3].)

**Definition 10.1.** Let  $R$  be a  $\sigma$ -ring and  $\mathfrak{a} \subset R$  a  $\sigma$ -ideal. Then  $\mathfrak{a}$  is called

- reflexive if  $\sigma^{-1}(\mathfrak{a}) = \mathfrak{a}$ , i.e.,  $\sigma(f) \in \mathfrak{a}$  implies  $f \in \mathfrak{a}$ .
- mixed if  $fg \in \mathfrak{a}$  implies  $f\sigma(g) \in \mathfrak{a}$ .
- perfect if  $\sigma^{\alpha_1}(f) \cdots \sigma^{\alpha_n}(f) \in \mathfrak{a}$  implies  $f \in \mathfrak{a}$  for  $\alpha_1, \dots, \alpha_n \geq 0$

A  $\sigma$ -ring whose zero ideal is reflexive / mixed / perfect is called  $\sigma$ -reduced / well-mixed / perfectly  $\sigma$ -reduced. Note that a  $\sigma$ -ring which is an integral domain is well-mixed. If it is additionally  $\sigma$ -reduced, i.e., a  $\sigma$ -domain, it is perfectly  $\sigma$ -reduced.

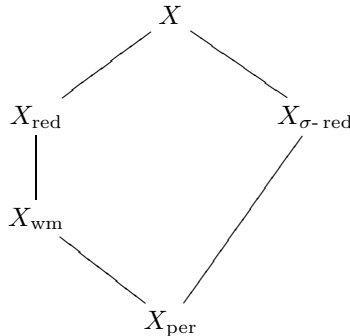
Let  $\mathfrak{a}$  be a  $\sigma$ -ideal of a  $\sigma$ -ring  $R$ . Since the intersection of reflexive / radical mixed / perfect  $\sigma$ -ideals is a reflexive / radical mixed / perfect  $\sigma$ -ideal there exists a smallest reflexive / radical mixed / perfect  $\sigma$ -ideal of  $R$  containing  $\mathfrak{a}$ . It is called the reflexive closure  $\mathfrak{a}^*$  / the radical mixed closure  $\{\mathfrak{a}\}_{\text{wm}}$  / the perfect closure  $\{\mathfrak{a}\}$  of  $\mathfrak{a}$ .

Let  $X$  be a  $\sigma$ -variety. We say that  $X$  is reduced /  $\sigma$ -reduced / reduced well-mixed / perfectly  $\sigma$ -reduced if  $k\{X\}$  has this property. There exists a unique largest  $\sigma$ -closed  $\sigma$ -subvariety

$$X_{\text{red}} / X_{\sigma\text{-red}} / X_{\text{wm}} / X_{\text{per}}$$

of  $X$  which is reduced /  $\sigma$ -reduced / reduced well-mixed / perfectly  $\sigma$ -reduced. Its defining ideal is the radical / reflexive closure / radical mixed closure / perfect closure of the zero ideal of  $k\{X\}$ .

A perfect  $\sigma$ -ideal is reduced, mixed and reflexive. Therefore we have the following diagram of inclusions of  $\sigma$ -closed  $\sigma$ -subvarieties of  $X$ .



The importance of perfectly  $\sigma$ -reduced  $\sigma$ -varieties stems from the fact that they correspond to the classical difference varieties as studied in [Coh65] and [Lev08], where one is only looking for solutions in  $\sigma$ -field extensions of  $k$ . Mixed  $\sigma$ -ideals play a crucial role in the theory of difference schemes as developed by E. Hrushovski in [Hru04]. Note that for an arbitrary non-empty  $\sigma$ -variety  $X_{\text{per}}$  and  $X_{\text{wm}}$  might be empty. Take for example  $k\{X\} = k \times k$  with  $\sigma((a, b)) = (\sigma(b), \sigma(a))$ . This pathology does not occur for  $\sigma$ -algebraic groups since the kernel of the counit  $\varepsilon: k\{G\} \rightarrow k$  is a  $\sigma$ -prime ideal.



**Example 10.2.** Let  $k$  be a  $\sigma$ -field,  $G$  a finite group and  $\Sigma: G \rightarrow G$  a group endomorphism. Let  $G$  be the  $\sigma$ -algebraic group from Example 2.12. Then  $G$  is  $\sigma$ -reduced if and only if  $\Sigma$  is an automorphism. Moreover,  $G$  is reduced well-mixed if and only if it is perfectly  $\sigma$ -reduced if and only if  $\Sigma$  is the identity map.

**Remark 10.3.** For a  $\sigma$ -algebraic group  $G$  the following statements are equivalent:

- (i)  $G(K) = 1$  for every  $\sigma$ -field extension  $K$  of  $k$ .
- (ii)  $G_{\text{per}} = 1$ .
- (iii) The kernel of the counit  $k\{G\} \rightarrow k$  is the only  $\sigma$ -prime ideal of  $k\{G\}$ .

*Proof.* This follows from the fact that a perfect difference ideal is the intersection of  $\sigma$ -prime ideals ([Coh65, Chapter 3, p. 88]).  $\square$

**Remark 10.4.** If  $G$  is a  $\sigma$ -algebraic group such that  $k\{G\}$  is well-mixed, then  $G$  has only finitely many components and they are all  $\sigma$ -components. If  $G$  is a  $\sigma$ -algebraic group such that  $G_{\text{wm}}$  is a  $\sigma$ -closed subgroup of  $G$  (e.g.,  $k$  is algebraically closed, see Corollary 10.8), then the  $\sigma$ -components of  $G$  are in bijection with the components of  $G_{\text{wm}}$ .

*Proof.* By [Hru04, Lemma 2.10] a radical mixed  $\sigma$ -ideal is the intersection of prime  $\sigma$ -ideals. If  $k\{G\}$  is well-mixed, the nilradical of  $k\{G\}$  is mixed and therefore it is the intersection of the minimal prime  $\sigma$ -ideals. Since there are only finitely many minimal prime  $\sigma$ -ideals in  $k\{G\}$  (Theorem 9.1) we see that there are only finitely many minimal prime ideals in  $k\{G\}$  and all of them are  $\sigma$ -ideals.

Assume that  $G$  is a  $\sigma$ -algebraic group such that  $G_{\text{wm}}$  is a  $\sigma$ -closed subgroup of  $G$ . The set of minimal prime ideals of  $k\{G\}$  which are  $\sigma$ -ideals equals the set of minimal prime  $\sigma$ -ideals of  $k\{G\}$  (Corollary 9.8) and the latter is the set of all prime ideals of  $k\{G\}$  which are minimal above  $\{0\}_{\text{wm}}$ .  $\square$

If  $\psi: R \rightarrow S$  is a morphism of  $\sigma$ -rings, it is easy to check that  $\psi^{-1}(\mathfrak{a})$  is a radical / reflexive / radical mixed / perfect  $\sigma$ -ideal if  $\mathfrak{a}$  has the corresponding property. This shows that  $\psi$  maps the radical / reflexive closure / radical mixed closure / perfect closure of the zero ideal of  $R$  into the radical / reflexive closure / radical mixed closure / perfect closure of the zero ideal of  $S$ . Therefore a morphism of  $\sigma$ -varieties  $X \rightarrow Y$  induces a morphism

$$X_{\text{red}} \rightarrow Y_{\text{red}} / X_{\sigma\text{-red}} \rightarrow Y_{\sigma\text{-red}} / X_{\text{wm}} \rightarrow Y_{\text{wm}} / X_{\text{per}} \rightarrow Y_{\text{per}}.$$

For later use we record a lemma on perfectly  $\sigma$ -reduced  $\sigma$ -varieties.

**Lemma 10.5.** Let  $\phi: X \rightarrow Y$  be a morphism of  $\sigma$ -varieties and let  $Z \subset Y$  be a  $\sigma$ -closed  $\sigma$ -subvariety. Assume that  $X$  is perfectly  $\sigma$ -reduced. If  $\phi_K(X(K)) \subset Z(K)$  for every  $\sigma$ -field extension  $K$  of  $k$ , then  $\phi(X) \subset Z$ , i.e.,  $\phi$  factors through  $Z \hookrightarrow Y$ .

*Proof.* We have to show that  $\mathbb{I}(Z) \subset k\{Y\}$  lies in the kernel of  $\phi^*: k\{Y\} \rightarrow k\{X\}$ . So let  $f \in \mathbb{I}(X)$ . We have to show that  $\phi^*(f) = 0$ . Since the zero ideal of  $k\{X\}$  is perfect, it is the intersection of  $\sigma$ -prime ideals ([Coh65, Chapter 3, p. 88]). Therefore, it suffices to show that  $\phi^*(f)$  lies in every  $\sigma$ -prime ideal of  $k\{X\}$ . Let  $\mathfrak{p} \subset k\{X\}$  be a  $\sigma$ -prime ideal, then the field of fractions  $K$  of  $k\{X\}/\mathfrak{p}$  naturally is a  $\sigma$ -field and the canonical map  $x: k\{X\} \rightarrow K$  is a morphism of  $k$ - $\sigma$ -algebras. By assumption,  $\phi_K(x) \in Z(K)$ , i.e.,  $\mathbb{I}(Z)$  lies in the kernel of  $x \circ \phi^*$ . So  $\phi^*(f) \in \mathfrak{p}$ .  $\square$

**Lemma 10.6.** Let  $R$  and  $S$  be  $k$ - $\sigma$ -algebras.

- (i) If  $k$  is perfect and  $R$  and  $S$  are reduced, then  $R \otimes_k S$  is reduced.
- (ii) If  $k$  is inversive and  $R$  and  $S$  are  $\sigma$ -reduced, then  $R \otimes_k S$  is  $\sigma$ -reduced.
- (iii) If  $k$  is algebraically closed and  $R$  and  $S$  are well-mixed and reduced, then  $R \otimes_k S$  is well-mixed and reduced.
- (iv) If  $k$  is inversive and algebraically closed and  $R$  and  $S$  are perfectly  $\sigma$ -reduced, then  $R \otimes_k S$  is perfectly  $\sigma$ -reduced.

*Proof.* Of course (i) is well-known. See e.g., [Bou90, Theorem 3, Chapter V, §15.5, A.V.125]. Note that (i) is a special case of (ii) as we may take  $\sigma$  as the Frobenius endomorphism. For (ii), first note that if  $(r_i)_{i \in I}$  is a  $k$ -basis of  $R$ , then  $(\sigma(r_i))_{i \in I}$  is  $k$ -linearly independent: If  $\sum \lambda_i \sigma(r_i) = 0$  we can write  $\lambda_i = \sigma(\mu_i)$  as  $k$  is inversive and then  $0 = \sigma(\sum \mu_i r_i)$  implies  $\sum \mu_i r_i = 0$  as  $R$  is  $\sigma$ -reduced. So  $\mu_i = 0$  and therefore  $\lambda_i = 0$  as claimed. Now let  $f = \sum r_i \otimes s_i \in R \otimes_k S$  with  $\sigma(f) = 0$ . Then  $\sum \sigma(r_i) \otimes \sigma(s_i) = 0$ . But since  $(\sigma(r_i))_{i \in I}$  is  $k$ -linearly independent this implies  $\sigma(s_i) = 0$  for all  $i \in I$ . As  $S$  is  $\sigma$ -reduced it follows that  $f = 0$ .

For (iii), note that the zero ideal of a reduced well-mixed  $\sigma$ -ring is the intersection of prime  $\sigma$ -ideals ([Hru04, Lemma 2.10]). If  $\mathfrak{p}$  is a prime  $\sigma$ -ideal of  $R$  and  $\mathfrak{q}$  a prime  $\sigma$ -ideal of  $S$ , then  $\mathfrak{p} \otimes S + R \otimes \mathfrak{q}$  is a prime  $\sigma$ -ideal of  $R \otimes_k S$  since

$$(R \otimes_k S)/(\mathfrak{p} \otimes S + R \otimes \mathfrak{q}) = R/\mathfrak{p} \otimes_k S/\mathfrak{q}$$

and the latter is an integral domain, as the tensor product of integral domains over an algebraically closed field is again an integral domain ([Bou90, Corollary 3, Chapter V, §17.5, A.V.143]). We see that the zero ideal of  $R \otimes_k S$  is the intersection of prime  $\sigma$ -ideals of the form  $\mathfrak{p} \otimes S + R \otimes \mathfrak{q}$ . This shows that  $R \otimes_k S$  is well-mixed and reduced.

To prove (iv) we can proceed as in (iii) by noting that a  $\sigma$ -ideal is perfect if and only if it is the intersection of  $\sigma$ -prime ideals and that the tensor product of  $\sigma$ -domains over an inversive algebraically closed  $\sigma$ -field is again a  $\sigma$ -domain by (ii).  $\square$

There are counterexamples which show that the conditions on the base  $\sigma$ -field in Lemma 10.6 can not be relaxed. For example, take  $k = \mathbb{R}$  with  $\sigma$  the identity map,  $R = \mathbb{C}$  with the identity map and  $S = \mathbb{C}$  with  $\sigma$  complex conjugation. Then  $R$  and  $S$  are perfectly  $\sigma$ -reduced (hence well-mixed) but  $R \otimes_k S$  is not well-mixed (hence not perfectly  $\sigma$ -reduced).

If  $X$  and  $Y$  are  $\sigma$ -varieties, the canonical map  $(X \times Y)_{\text{per}} \rightarrow X_{\text{per}} \times Y_{\text{per}}$  need not be an isomorphism as  $X_{\text{per}} \times Y_{\text{per}}$  need not be perfectly  $\sigma$ -reduced.

**Corollary 10.7.** *Let  $X$  and  $Y$  be  $\sigma$ -varieties.*

- (i) *If  $k$  is perfect, then  $(X \times Y)_{\text{red}} \simeq X_{\text{red}} \times Y_{\text{red}}$ .*
- (ii) *If  $k$  is inversive, then  $(X \times Y)_{\sigma\text{-red}} \simeq X_{\sigma\text{-red}} \times Y_{\sigma\text{-red}}$ .*
- (iii) *If  $k$  is algebraically closed, then  $(X \times Y)_{\text{wm}} \simeq X_{\text{wm}} \times Y_{\text{wm}}$ .*
- (iv) *If  $k$  is inversive and algebraically closed, then  $(X \times Y)_{\text{per}} \simeq X_{\text{per}} \times Y_{\text{per}}$ .*

*Proof.* Exemplarily, let us proof (iv). In terms of  $k$ - $\sigma$ -algebras, we have to show that the canonical map

$$k\{X\}/\{0\} \otimes_k k\{Y\}/\{0\} \rightarrow (k\{X\} \otimes_k k\{Y\})/\{0\}$$

is an isomorphism. As the left hand side is perfectly  $\sigma$ -reduced by Lemma 10.6, we see that  $\{0\} = \{0\} \otimes k\{Y\} + k\{X\} \otimes \{0\}$ .  $\square$

**Corollary 10.8.** *Let  $G$  be a  $\sigma$ -algebraic group.*

- (i) *If  $k$  is perfect, then  $G_{\text{red}}$  is a  $\sigma$ -closed subgroup of  $G$ .*
- (ii) *If  $k$  is inversive, then  $G_{\sigma\text{-red}}$  is a  $\sigma$ -closed subgroup of  $G$ .*
- (iii) *If  $k$  is algebraically closed, then  $G_{\text{wm}}$  is a  $\sigma$ -closed subgroup of  $G$ .*
- (iv) *If  $k$  is inversive and algebraically closed, then  $G_{\text{per}}$  is a  $\sigma$ -closed subgroup of  $G$ .*

*Proof.* Again, let us restrict to (iv). The other cases are similar. The multiplication morphism  $G \times G \rightarrow G$  induces a morphism  $(G \times G)_{\text{per}} \rightarrow G_{\text{per}}$ . But by Corollary 10.7, the  $\sigma$ -closed  $\sigma$ -subvariety  $(G \times G)_{\text{per}}$  of  $G \times G$  can be identified with  $G_{\text{per}} \times G_{\text{per}} \subset G \times G$ . Therefore, the multiplication maps  $G_{\text{per}} \times G_{\text{per}}$  into  $G_{\text{per}}$ . As the inversion  $G \rightarrow G$ ,  $g \mapsto g^{-1}$  also passes to  $G_{\text{per}}$ , we see that  $G_{\text{per}}$  is a subgroup of  $G$ .  $\square$

**Example 10.9.** For all the  $\sigma$ -algebraic groups  $G$  in the list before Lemma 9.3  $G_{\text{per}}$  is the trivial group.

The following example shows that  $G_{\sigma\text{-red}}$  need to be a subgroup if  $k$  is not inversive.

**Example 10.10.** Let  $k$  be a  $\sigma$ -field of characteristic zero which is not inversive. So there exists  $\lambda \in k$  with  $\lambda \notin \sigma(k)$ . Let  $G$  be the  $\sigma$ -closed subgroup of  $\mathbb{G}_a$  given by

$$G(R) = \{g \in R \mid \sigma^2(g) + \lambda\sigma(g) = 0\}$$

for any  $k$ - $\sigma$ -algebra  $R$ . We will show that  $G$  has no proper, non-trivial  $\sigma$ -closed subgroup. Suppose that  $H$  is a proper, non-trivial  $\sigma$ -closed subgroup of  $G$ . By Corollary A.3 in [DVHW] every  $\sigma$ -closed subgroup of  $\mathbb{G}_a$  is of the form  $\mathbb{V}(f)$ , where  $f \in k\{y\}$  is the unique monic linear homogeneous difference polynomial of minimal order in  $\mathbb{I}(H) \subset k\{\mathbb{G}_a\} = k\{y\}$ . As  $H$  is non-trivial and properly contained in  $G$ ,  $f$  must have order one, i.e.,  $f = \sigma(y) + \mu y$  for some  $\mu \in k$ . But then  $\sigma^2(h) + \sigma(\mu)\sigma(h) = 0$  and therefore  $(\lambda - \sigma(\mu))h = 0$  for all  $h \in H(R)$  for any  $k$ - $\sigma$ -algebra  $R$ . Thus  $\lambda = \sigma(\mu)$ ; a contradiction.

Now assume that  $\lambda^2 \in \sigma(k)$ . (For example, we can choose  $k = \mathbb{C}(\sqrt{x}, \sqrt{x+1}, \dots)$  with action of  $\sigma$  determined by  $\sigma(x) = x+1$  and  $\lambda = \sqrt{x}$ .) We have  $k\{G\} = k[y, \sigma(y)]$  and if we choose  $\eta \in k$  such that  $\sigma(\eta) = \lambda^2$ , then  $\sigma(y)^2 - \eta y^2$  lies in the reflexive closure of the zero ideal of  $k\{G\}$ . As  $y$  does not lie in the reflexive closure of the zero ideal,  $G_{\sigma\text{-red}}$  is not the trivial group but properly contained in  $G$ . So, by the above,  $G_{\sigma\text{-red}}$  can not be a subgroup.

The following example shows that the  $\sigma$ -closed subgroups constructed in Corollary 10.8 are in general not normal.

**Example 10.11.** Let  $N$  be the  $\sigma$ -closed subgroup of  $\mathbb{G}_a$  given by  $N(R) = \{g \in R \mid \sigma(g) = 0\}$  for any  $k$ - $\sigma$ -algebra  $R$ . The  $\sigma$ -algebraic group  $H = \mathbb{G}_m$  acts on  $N$  by group automorphisms

$$H(R) \times N(R) \rightarrow N(R), (h, n) \mapsto hn.$$

So we can form the semidirect product  $G = N \rtimes H$  which is the  $\sigma$ -variety  $G \times N$  with group multiplication given by

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 + h_1 n_2, h_1 h_2).$$

Then  $k\{G\} = k\{N\} \otimes_k k\{H\} = k[x] \otimes_k k\{y, y^{-1}\}$  with  $\sigma(x) = 0$ . The reflexive closure of the zero ideal of  $k\{G\}$  is the ideal of  $k\{G\}$  generated by  $x$ . Therefore  $G_{\sigma\text{-red}} = H \leq G$ . For  $h \in H(R)$  and  $n \in N(R)$  we have

$$(n, 1)(0, h)(n, 1)^{-1} = (n - hn, h)$$

which shows that  $G_{\sigma\text{-red}}$  is not normal in  $G$ .

In the following lemma we tacitly assume that  $k$  has the relevant properties as stated in Corollary 10.8, so that we are dealing with  $\sigma$ -closed subgroups.

**Lemma 10.12.** *Let  $G$  be a  $\sigma$ -algebraic group. Then  $\sigma\text{-dim}(G_{\text{red}})$ ,  $\sigma\text{-dim}(G_{\sigma\text{-red}})$ ,  $\sigma\text{-dim}(G_{\text{wm}})$  and  $\sigma\text{-dim}(G_{\text{per}})$  are all equal to  $\sigma\text{-dim}(G)$ .*

*Proof.* As the dimension of a finitely generated  $k$ -algebra remains invariant if we factor by the nilradical, it follows easily that  $\sigma\text{-dim}(G_{\text{red}}) = \sigma\text{-dim}(G)$ .

Since  $(G^o)_{\sigma\text{-red}} \leq G_{\sigma\text{-red}}$ ,  $(G^o)_{\text{wm}} \leq G_{\text{wm}}$  and  $(G^o)_{\text{per}} \leq G_{\text{per}}$  we may assume that  $G$  is connected by Lemma 9.18. But then the nilradical of  $k\{G\}$  is a prime  $\sigma$ -ideal (Proposition 9.14) and therefore  $G_{\text{wm}} = G_{\text{red}}$  and thus  $\sigma\text{-dim}(G_{\text{wm}}) = \sigma\text{-dim}(G)$  also in this case.

To prove  $\sigma\text{-dim}(G_{\text{per}}) = \sigma\text{-dim}(G)$  we may assume that  $G$  is reduced. Then the zero ideal of  $k\{G\}$  is prime and therefore its reflexive closure  $\cup_{i \geq 1} \sigma^{-i}(0)$  is a  $\sigma$ -prime ideal. This shows that  $G_{\text{per}} = G_{\sigma\text{-red}}$ .

It thus suffices to show that  $\sigma\text{-dim}(G_{\sigma\text{-red}}) = \sigma\text{-dim}(G)$ . Let  $\mathcal{G}$  be an algebraic group containing  $G$  as a  $\sigma$ -closed subgroup and for  $i \geq 0$  let  $G[i]$  and  $G_{\sigma\text{-red}}[i]$  denote the  $i$ -th order Zariski closure of  $G$  and  $G_{\sigma\text{-red}}$  in  $\mathcal{G}$  respectively. By Corollary 4.2 there exists  $m \geq 0$  such that

$$\mathbb{I}(G_{\sigma\text{-red}}[i]) = (\mathbb{I}(G_{\sigma\text{-red}}[i-1]), \sigma(\mathbb{I}(G_{\sigma\text{-red}}[i-1]))) \subset k[G[i]] \subset k\{G\}$$

for  $i > m$ . But  $\mathbb{I}(G_{\sigma\text{-red}}) \subset k\{G\}$  is the reflexive closure of the zero ideal and so  $\mathbb{I}(G_{\sigma\text{-red}}) = \{f \in k\{G\} \mid \exists n \geq 1 : \sigma^n(f) = 0\}$  (cf. [Lev08, p. 107]). This shows that there exist  $f_1, \dots, f_m$  in  $k\{G\}$  such that  $\mathbb{I}(G_{\sigma\text{-red}}[i]) = (f_1, \dots, f_m) \subset k[G[i]]$  for  $i \gg 0$ . Therefore  $\dim(G[i]) - \dim(G_{\sigma\text{-red}}[i]) \leq m$  for  $i \gg 0$  and consequently  $\sigma\text{-dim}(G) = \sigma\text{-dim}(G_{\sigma\text{-red}})$ .  $\square$

Note that the order of  $G_{\sigma\text{-red}}$  might be strictly smaller than the order of  $G$ . This for example is the case for  $G \leq \mathbb{G}_a$  given by  $G(R) = \{g \in R \mid \sigma(g) = 0\}$  for any  $k$ - $\sigma$ -algebra  $R$ .

## 11 Group theory

Ultimately the goal of this section is to prove the analogs of the (Noether) isomorphism theorems for groups. This task is complicated by the fact that for a normal  $\sigma$ -closed subgroup  $N$  of a  $\sigma$ -algebraic group  $G$ , the quotient  $G/N$  is, at least initially, not easily accessible. As for algebraic groups, the functor  $R \rightsquigarrow G(R)/N(R)$  need not be representable, in particular, it is distinct from  $G/N$ .

If we could identify  $G$  with  $G(k)$ , and  $(G/N)(k)$  with  $G(k)/N(k)$ , where  $k$  is some “sufficiently large” difference field, we could apply the isomorphism theorems directly. This approach is not possible for us for several reasons. Firstly, we want to avoid restrictions on the base field. Secondly, the identification of  $G$  with  $G(k)$  is only feasible for perfectly  $\sigma$ -reduced  $\sigma$ -algebraic groups. Thirdly, identifying  $G$  with  $G(k)$  does introduce some blemishes. For example, the morphism of  $\sigma$ -algebraic groups  $\phi: \mathrm{GL}_n \rightarrow \mathrm{GL}_n$ ,  $g \mapsto \sigma(g)$  is such that  $\phi_k: \mathrm{GL}_n(k) \rightarrow \mathrm{GL}_n(k)$  has trivial kernel, but  $\phi$  is not a  $\sigma$ -closed embedding. Indeed, the kernel of  $\phi$  is non-trivial.

For algebraic groups, the theory of sheaves (see [DG70, Chapter III]) provides an elegant and powerful tool to deal with quotients. In the first part of this section we adapt the theory of sheaves to difference algebra. The main result (Theorem 11.8) provides a canonical way to associate a sheaf to any functor from  $k$ - $\sigma$ -Alg to Sets. The relevance of Theorem 11.8 for quotients stems from the fact that the sheaf associated to the functor  $R \rightsquigarrow G(R)/N(R)$  equals  $G/N$ . In the second part we then show how this result can be used to deduce the isomorphism theorems for difference algebraic groups from the isomorphism theorems for (abstract) groups. While it may be possible to prove the isomorphism theorems for difference algebraic groups without explicitly introducing sheaves, we expect that Theorem 11.8 will also be useful in other situations, for example, when considering actions of difference algebraic groups on difference varieties, where the existence of a quotient in the category of difference varieties is problematic.

### 11.1 Sheaves

Our proof of Theorem 11.8 follows the proof of Theorem 1.8, Chapter III, §1 [DG70] rather closely.

Let  $k$  be a  $\sigma$ -field. If  $(R_i)_{i \in I}$  is a finite family of  $k$ - $\sigma$ -algebras, then the product  $\prod_{i \in I} R_i$  is naturally a  $k$ - $\sigma$ -algebra by  $\sigma((r_i)_{i \in I}) = (\sigma(r_i))_{i \in I}$ . The projections  $\prod_{i \in I} R_i \rightarrow R_i$  are morphisms of  $k$ - $\sigma$ -algebras. Recall that a morphism  $\psi: R \rightarrow S$  of  $k$ - $\sigma$ -algebras is called faithfully flat if the corresponding morphism  $\psi^\#: R^\# \rightarrow S^\#$  of  $k$ -algebras is faithfully flat.

**Definition 11.1.** *Let  $R$  be a  $k$ - $\sigma$ -algebra. A finite family  $(R_i)_{i \in I}$  of  $R$ - $\sigma$ -algebras is called  $R$ -covering if the canonical map  $R \rightarrow \prod_{i \in I} R_i$  is faithfully flat.*

Note that if  $(R_i)_{i \in I}$  and  $(S_j)_{j \in J}$  are two  $R$ -covering families, then  $(R_i \otimes_R S_j)_{(i,j) \in I \times J}$  is an  $R$ -covering family. If  $R \rightarrow S$  is a morphism of  $k$ - $\sigma$ -algebras and  $(R_i)_{i \in I}$  is an  $R$ -covering family, then  $(R_i \otimes_R S)_{i \in I}$  is an  $S$ -covering family.

Recall that a sequence of sets  $A \xrightarrow{\alpha} B \begin{smallmatrix} \xrightarrow{\beta_1} \\ \xrightarrow{\beta_2} \end{smallmatrix} C$  is called exact if  $\alpha$  is the equalizer of  $\beta_1$  and  $\beta_2$ , i.e.,  $\beta_1 \alpha = \beta_2 \alpha$  and for  $b \in B$  with  $\beta_1(b) = \beta_2(b)$  there exists a unique  $a \in A$  with  $\alpha(a) = b$ .

**Definition 11.2.** *Let  $F$  be a functor from  $k$ - $\sigma$ -Alg to Sets. Then  $F$  is called a sheaf, if for every  $k$ - $\sigma$ -algebra  $R$  and every  $R$ -covering family  $(R_i)_{i \in I}$  the sequence*

$$F(R) \xrightarrow{\alpha} \prod_i F(R_i) \begin{smallmatrix} \xrightarrow{\beta_1} \\ \xrightarrow{\beta_2} \end{smallmatrix} \prod_{i,j} F(R_i \otimes_R R_j) \quad (16)$$

*is exact.*

The maps in the above sequence are the obvious ones: The  $i$ -th component of  $\alpha$  is induced from  $R \rightarrow R_i$ . The  $(i, j)$ -component of  $\beta_1$  (respectively  $\beta_2$ ) is the projection onto  $F(R_i)$  (respectively  $F(R_j)$ ) followed by the map induced from  $R_i \rightarrow R_i \otimes_R R_j$ ,  $f \mapsto f \otimes 1$  (respectively  $R_j \rightarrow R_i \otimes_R R_j$ ,  $f \mapsto 1 \otimes f$ ).

A morphism of sheaves is a morphism of functors.

**Lemma 11.3.** *A functor  $F$  from  $k$ - $\sigma$ -Alg to Sets is a sheaf if and only if*

- (i) *for every finite family of  $k$ - $\sigma$ -algebras  $(R)_{i \in I}$ , the map  $F(\prod_{i \in I} R_i) \rightarrow \prod_{i \in I} F(R_i)$  is bijective;*

(ii) for every faithfully flat morphism of  $k$ - $\sigma$ -algebras  $R \rightarrow S$  the sequence

$$F(R) \rightarrow F(S) \rightrightarrows F(S \otimes_R S)$$

is exact.

*Proof.* Let us first assume that  $F$  is a sheaf. If we take  $R$  as the zero ring and the  $R$ -covering family as the empty family, then the exactness of (16) signifies that  $F(R)$  consists of one element.

Let  $(R_i)_{i \in I}$  be a finite family of  $k$ - $\sigma$ -algebras. If we set  $R = \prod_i R_i$  and consider  $R_i$  as a  $R$ - $\sigma$ -algebra via the projection  $R \rightarrow R_i$ , then the canonical map  $R \rightarrow \prod_i R_i$  is the identity and  $R_i \otimes_R R_j = 0$  for  $i \neq j$ , whereas  $R_i \otimes_R R_j = R_i$  for  $i = j$ . Thus the exactness of (16) in this case yields condition (i) since  $\beta_1$  and  $\beta_2$  are reduced to the identity map. Clearly a sheaf satisfies condition (ii).

Conversely, assume that  $F$  satisfies (i) and (ii). Let  $(R_i)_{i \in I}$  be an  $R$ -covering family. Taking  $S = \prod R_i$  and applying (i) to (ii) yields the exactness of (16).  $\square$

**Corollary 11.4.** *Every representable functor from  $k$ - $\sigma$ -Alg to Sets is a sheaf. In particular, every  $\sigma$ -variety and every  $\sigma$ -algebraic group is a sheaf.*

*Proof.* Let  $A$  be a  $k$ - $\sigma$ -algebra and  $F = \text{Hom}(A, -)$ . Clearly,

$$\text{Hom}(A, \prod_i R_i) \simeq \prod_i \text{Hom}(A, R_i),$$

for every finite family  $(R_i)_{i \in I}$  of  $k$ - $\sigma$ -algebras. So  $F$  satisfies condition (i) of Lemma 11.3.

To verify (ii), let  $R \rightarrow S$  be a faithfully flat morphism of  $k$ - $\sigma$ -algebras. Then

$$R \rightarrow S \rightrightarrows S \otimes_R S$$

is exact. (See e.g. [Wat79, Section 13.1, p. 104].) Therefore

$$\text{Hom}(A, R) \rightarrow \text{Hom}(A, S) \rightrightarrows \text{Hom}(A, S \otimes_R S)$$

is exact.  $\square$

Thus the category of  $\sigma$ -varieties is a full subcategory of the category of sheaves.

**Definition 11.5.** *A subfunctor  $D$  of a functor  $F: k\text{-}\sigma\text{-Alg} \rightarrow \text{Sets}$  is called fat if for every  $k$ - $\sigma$ -algebra  $R$  and every  $a \in F(R)$  there exists an  $R$ -covering family  $(R_i)_{i \in I}$  such that the image of  $a$  in  $F(R_i)$  belongs to  $D(R_i)$  for every  $i \in I$ .*

Some of the constructions with  $\sigma$ -varieties explained in Section 1 carry over to arbitrary functors from  $k$ - $\sigma$ -Alg to Sets without difficulty: If  $\phi: E \rightarrow F$  is a morphism of functors and  $D \subset F$  a subfunctor, then  $\text{Im}(\phi)$  and  $\phi^{-1}(D)$  may be defined as in Section 1; similarly for the intersection of subfunctors.

Note that if  $\phi: E \rightarrow F$  is a morphism of functors and  $D \subset F$  is fat, then  $\phi^{-1}(D) \subset E$  is fat. As in [DG70, p. 285] one verifies: If  $D$  is a fat subfunctor of  $F$  and  $D_1$  is a fat subfunctor of  $D$ , then  $D_1$  is a fat subfunctor of  $F$ . If  $D_1$  and  $D_2$  are fat subfunctors of  $E$ , then  $D_1 \cap D_2$  is a fat subfunctor of  $E$ .

Let  $R$  be a  $k$ - $\sigma$ -algebra. To simplify the notation we will write

$$\text{Sp}^\sigma(R)$$

for the functor  $\text{Hom}(R, -): k\text{-}\sigma\text{-Alg} \rightarrow \text{Sets}$ . If  $\psi: R \rightarrow S$  is a morphism of  $k$ - $\sigma$ -algebras, there is an induced morphism of functors  $\text{Sp}^\sigma(\psi): \text{Sp}^\sigma(S) \rightarrow \text{Sp}^\sigma(R)$ . Recall (See e.g. [EH00, Lemma VI-1 (a)].) that for any functor  $F: k\text{-}\sigma\text{-Alg} \rightarrow \text{Sets}$  and any  $k$ - $\sigma$ -algebra  $R$  there is a canonical bijection

$$F(R) \simeq \text{Hom}(\text{Sp}^\sigma(R), F)$$

Indeed,  $F$  and  $\text{Hom}(\text{Sp}^\sigma(-), F)$  are isomorphic as functors. An element  $a \in F(R)$  gives rise to morphism  $\text{Sp}^\sigma(R) \rightarrow F$  as follows: For a  $k$ - $\sigma$ -algebra  $S$  and  $\psi \in \text{Hom}(R, S)$  let  $\text{Sp}^\sigma(R)(S) \rightarrow F(S)$  be defined by sending  $\psi$  to  $F(\psi)(a)$ . Conversely, from a morphism  $\text{Sp}^\sigma(R) \rightarrow F$  we obtain an element in  $F(R)$  by considering the image of the identity under  $\text{Sp}^\sigma(R)(R) \rightarrow F(R)$ .

**Lemma 11.6.** *Let  $R$  be a  $k$ - $\sigma$ -algebra. Then a subfunctor  $D$  of  $\text{Sp}^\sigma(R)$  is fat if and only if there exists an  $R$ -covering family  $(R_i)_{i \in I}$  such that  $\text{Im}(\text{Sp}^\sigma(R_i) \rightarrow \text{Sp}^\sigma(R)) \subset D$  for all  $i \in I$ .*

*Proof.* If  $D \subset \text{Sp}^\sigma(R)$  is fat, we can apply Definition 11.5 to the element  $a = \text{id}_R \in \text{Hom}(R, R) = \text{Sp}^\sigma(R)(R)$  to find an  $R$ -covering family  $(R_i)_{i \in I}$  such that the maps  $R \rightarrow R_i$  lie in  $D(R_i) \subset \text{Sp}^\sigma(R)(R_i)$  for every  $i \in I$ . Let  $\psi: R_i \rightarrow S$  be a morphism of  $k$ - $\sigma$ -algebras. Since  $\text{Sp}^\sigma(R)(\psi): \text{Sp}^\sigma(R)(R_i) \rightarrow \text{Sp}^\sigma(R)(S)$  maps  $D(R_i)$  into  $D(S)$  we see that the composition  $R \rightarrow R_i \rightarrow S$  lies in  $D(S) \subset \text{Sp}^\sigma(R)(S)$ . Therefore the image of  $\text{Sp}^\sigma(R_i)(S) \rightarrow \text{Sp}^\sigma(R)(S)$  lies in  $D(S)$ , i.e.,  $\text{Im}(\text{Sp}^\sigma(R_i) \rightarrow \text{Sp}^\sigma(R)) \subset D$ .

Conversely, if  $(R_i)_{i \in I}$  verifies the condition of the lemma and  $a: R \rightarrow S$  is a morphism of  $k$ - $\sigma$ -algebras, then  $(R_i \otimes_R S)_{i \in I}$  is an  $S$ -covering family. By assumption,  $R \rightarrow R_i \rightarrow R_i \otimes_R S$  lies in  $D(R_i \otimes_R S) \subset \text{Sp}^\sigma(R)(R_i \otimes_R S)$ . But  $R \rightarrow R_i \rightarrow R_i \otimes_R S$  equals  $R \rightarrow S \rightarrow R_i \otimes_R S$ . Therefore  $\text{Sp}^\sigma(R)(S) \rightarrow \text{Sp}^\sigma(R)(R_i \otimes_R S)$  maps  $a$  into  $D(R_i \otimes_R S)$ .  $\square$

**Proposition 11.7.** *For a functor  $F: k\text{-}\sigma\text{-Alg} \rightarrow \text{Sets}$  the following properties are equivalent:*

- (i) *The functor  $F$  is a sheaf.*
- (ii) *If  $D$  is a fat subfunctor of a functor  $E: k\text{-}\sigma\text{-Alg} \rightarrow \text{Sets}$  and  $\phi: D \rightarrow F$  a morphism, then there exists a unique extension of  $\phi$  to  $E$ .*
- (iii) *If  $R$  is a  $k$ - $\sigma$ -algebra,  $D$  a fat subfunctor of  $\text{Sp}^\sigma(R)$  and  $\phi: D \rightarrow F$  a morphism, then there exists a unique extension of  $\phi$  to  $\text{Sp}^\sigma(R)$ .*

*Proof.* Let us start with (i) $\Rightarrow$ (ii). Let  $R$  be a  $k$ - $\sigma$ -algebra and  $a \in E(R)$ . We have to construct  $\phi(a) \in F(R)$ . Since  $D$  is fat, there exists an  $R$ -covering family  $(R_i)_{i \in I}$  such that the image  $a_i$  of  $a$  in  $E(R_i)$  belongs to  $D(R_i)$ . Since  $a \in E(R)$  we see that  $(a_i)_{i \in I} \in \prod_i D(R_i) \subset \prod_i E(R_i)$  lies in the equalizer of the top row of

$$\begin{array}{ccc} \prod_i D(R_i) & \rightrightarrows & \prod_{i,j} D(R_i \otimes_R R_j) \\ \downarrow & & \downarrow \\ \prod_i F(R_i) & \rightrightarrows & \prod_{i,j} F(R_i \otimes_R R_j). \end{array}$$

Therefore  $(\phi(a_i))_{i \in I} \in \prod_i F(R_i)$  lies in the equalizer of the bottom row. Since  $F$  is a sheaf there exists a unique  $b \in F(R)$  mapping to  $(\phi(a_i))_{i \in I}$ . Set  $\phi(a) = b$ . We have to show that this definition does not depend on the choice of the  $R$ -covering family  $(R_i)_{i \in I}$ . So let  $(S_j)_{j \in J}$  be another  $R$ -covering family such that the image of  $a \in E(R)$  lies in  $D(S_j) \subset E(S_j)$  for every  $j \in J$ . Then the  $R$ -covering family  $(R_i \otimes_R S_j)_{(i,j) \in I \times J}$  also has the property that the image of  $a$  in  $E(R_i \otimes_R S_j)$  lies in  $D(R_i \otimes_R S_j)$  for  $(i,j) \in I \times J$ . Performing the above construction of  $\phi(a)$  with the  $R$ -covering family  $(R_i \otimes_R S_j)_{(i,j) \in I \times J}$  and considering the commutativity of

$$\begin{array}{ccc} & \prod_i R_i & \\ & \downarrow & \\ R & \xrightarrow{\quad} & \prod_{i,j} R_i \otimes_R S_j \\ & \uparrow & \\ & \prod_j S_j & \end{array}$$

we see that  $\phi(a)$  is well-defined. To show that the definition of  $\phi$  is functorial in  $R$  we can consider a morphism  $R \rightarrow S$  of  $k$ - $\sigma$ -algebras and the  $S$ -covering family  $(R_i \otimes_R S)_{i \in I}$ . The fact that  $\phi: E \rightarrow F$  is the unique extension of  $\phi: D \rightarrow F$  is immediate from the construction of  $\phi$ .

The implication (ii) $\Rightarrow$ (iii) is obvious. Thus it only remains to show that (iii) $\Rightarrow$ (i). Let  $(R_i)_{i \in I}$  be an  $R$ -covering family. Let  $D$  be the subfunctor of  $\text{Sp}^\sigma(R)$  equal to the union  $\cup_{i \in I} \text{Im}(\text{Sp}^\sigma(R_i) \rightarrow \text{Sp}^\sigma(R))$ , i.e., a morphism of  $k$ - $\sigma$ -algebras  $R \rightarrow S$  lies in  $D(S)$  if and only if it factors through  $R \rightarrow R_i$  for some  $i \in I$ . Then  $D$  is a fat subfunctor of  $\text{Sp}^\sigma(R)$  by Lemma 11.6. We claim that the sequence

$$\text{Hom}(D, F) \xrightarrow{\alpha} \prod_i \text{Hom}(\text{Sp}^\sigma(R_i), F) \xrightleftharpoons[\beta_2]{\beta_1} \prod_{i,j} \text{Hom}(\text{Sp}^\sigma(R_i \otimes_R R_j), F) \quad (17)$$

is exact. The injectivity of  $\alpha$  is clear from the definition of  $D$ . Let  $f = (f_i)_{i \in I} \in \prod_i \text{Hom}(\text{Sp}^\sigma(R_i), F)$  be such that  $\beta_1(f) = \beta_2(f)$ . Then for every pair  $(i, j) \in I \times I$

$$\begin{array}{ccc}
& \mathrm{Sp}^\sigma(R_i) \times_{\mathrm{Sp}^\sigma(R)} \mathrm{Sp}^\sigma(R_j) & \\
& \downarrow \simeq & \\
& \mathrm{Sp}^\sigma(R_i \otimes_R R_j) & \\
\swarrow & & \searrow \\
\mathrm{Sp}^\sigma(R_i) & & \mathrm{Sp}^\sigma(R_j) \\
\searrow f_i & & \swarrow f_j \\
& F(R) &
\end{array} \tag{18}$$

commutes. Let us define a morphism  $h: D \rightarrow F$  as follows: If  $S$  is a  $k$ - $\sigma$ -algebra and  $a \in D(S) \subset \mathrm{Sp}^\sigma(R)(S) = \mathrm{Hom}(R, S)$  then  $a$  factors as  $a: R \rightarrow R_i \xrightarrow{b} S$  for some  $i \in I$  and we can define  $h(a) = f_i(b) \in F(S)$ . It follows from the commutativity of (18) that  $h(a)$  does not depend on the choice of  $i$  and  $b$ . Clearly,  $\alpha(h) = f$ . Therefore (17) is exact.

By assumption, every morphism  $D \rightarrow F$  uniquely extends to  $\mathrm{Sp}^\sigma(R) \rightarrow F$ , i.e.,  $\mathrm{Hom}(\mathrm{Sp}^\sigma(R), F) \rightarrow \mathrm{Hom}(D, F)$  is bijective. Thus, applying the canonical bijections  $\mathrm{Hom}(\mathrm{Sp}^\sigma(S), F) \simeq F(S)$  to (17), yields the exactness of (16). So  $F$  is a sheaf.  $\square$

**Theorem 11.8.** *Let  $F$  be a functor from  $k$ - $\sigma$ -Alg to Sets. Then there exists a sheaf  $\tilde{F}$  and a morphism  $\iota: F \rightarrow \tilde{F}$  that is universal among morphisms from  $F$  to sheaves, i.e., for every morphism  $\phi$  from  $F$  to a sheaf  $E$  there exists a unique morphism  $\tilde{\phi}: \tilde{F} \rightarrow E$  making*

$$\begin{array}{ccc}
F & \xrightarrow{\iota} & \tilde{F} \\
\searrow \phi & & \swarrow \tilde{\phi} \\
& E &
\end{array}$$

commutative.

*Proof.* For any  $k$ - $\sigma$ -algebra  $R$  we set  $(\mathcal{L}F)(R) = \varinjlim \mathrm{Hom}(D, F)$ , where the limit is taken over all fat subfunctors  $D$  of  $\mathrm{Sp}^\sigma(R)$ . An element of  $(\mathcal{L}F)(R)$  is thus an equivalence class  $(D, \alpha)$ , where  $D$  is a fat subfunctor of  $\mathrm{Sp}^\sigma(R)$  and  $\alpha: D \rightarrow F$  a morphism of functors. We have  $(D, \alpha) = (D', \alpha')$  if and only if there exists a fat subfunctor  $D''$  of  $\mathrm{Sp}^\sigma(R)$  contained in  $D$  and  $D'$  such that the restrictions of  $\alpha$  and  $\alpha'$  to  $D''$  are equal.

Let  $\psi: R \rightarrow S$  be a morphism of  $k$ - $\sigma$ -algebras. For every fat subfunctor  $D$  of  $\mathrm{Sp}^\sigma(R)$  the map  $\mathrm{Sp}^\sigma(\psi): \mathrm{Sp}^\sigma(\psi)^{-1}(D) \rightarrow D$  induces a map  $\mathrm{Hom}(D, F) \rightarrow \mathrm{Hom}(\mathrm{Sp}^\sigma(\psi)^{-1}(D), F)$ . By passing to the limit we obtain a map  $\mathcal{L}(\psi): (\mathcal{L}F)(R) \rightarrow (\mathcal{L}F)(S)$ . Thus  $\mathcal{L}F$  is a functor from  $k$ - $\sigma$ -Alg to Sets. We have a morphism of functors  $\iota_F: F \rightarrow \mathcal{L}F$  determined by sending, for each  $k$ - $\sigma$ -algebra  $R$ , an element of  $F(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), F)$  to its canonical image in  $\varinjlim \mathrm{Hom}(D, F)$ .

Now set  $\tilde{F} = \mathcal{L}(\mathcal{L}F)$  and  $\iota = \iota_{\mathcal{L}F} \circ \iota_F$ . With the notation of the theorem, we will next show the existence and uniqueness of  $\tilde{\phi}$ . Since  $\iota = \iota_{\mathcal{L}F} \circ \iota_F$ , it suffices to show that for every morphism  $\phi$  from  $F$  to a sheaf  $E$ , there exists a unique morphism  $\phi': \mathcal{L}F \rightarrow E$  making

$$\begin{array}{ccc}
F & \xrightarrow{\iota_F} & \mathcal{L}F \\
\searrow \phi & & \swarrow \phi' \\
& E &
\end{array} \tag{19}$$

commutative.

Let us first prove the uniqueness of  $\phi'$ . Let  $R$  be a  $k$ - $\sigma$ -algebra and let  $\mu: \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$  correspond to  $(D, \alpha) \in (\mathcal{L}F)(R)$  under the bijection  $(\mathcal{L}F)(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), \mathcal{L}F)$ . It follows from the definitions that

$$\begin{array}{ccc}
D & \hookrightarrow & \mathrm{Sp}^\sigma(R) \\
\alpha \downarrow & & \downarrow \mu \\
F & \xrightarrow{\iota_F} & \mathcal{L}F
\end{array} \tag{20}$$

commutes. Let  $\eta: \mathrm{Sp}^\sigma(R) \rightarrow E$  correspond to  $\phi'((D, \alpha)) \in E(R)$  under the bijection  $E(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), E)$ . Then  $\eta = \phi'\mu$ . Combining this with (20) and (19), we see that the restriction of  $\eta$  to  $D$  equals  $\phi\alpha$ . By Proposition 11.7, this shows that  $\eta$  is uniquely determined by  $(D, \alpha)$  and  $\phi$ . Therefore  $\phi'((D, \alpha))$  is uniquely determined by  $\phi$ .

Let us now establish the existence of  $\phi'$ . Let  $R$  be a  $k$ - $\sigma$ -algebra and  $(D, \alpha) \in (\mathcal{L}F)(R)$ . By Proposition 11.7, the composition  $D \xrightarrow{\alpha} F \xrightarrow{\phi} E$  has a unique extension  $\eta: \mathrm{Sp}^\sigma(R) \rightarrow E$ . Note that  $\eta$  only depends on the equivalence class of  $D$  and  $\alpha$ . Now define  $\phi'((D, \alpha)) \in E(R)$  as the image of  $\eta$  under the canonical bijection  $\mathrm{Hom}(\mathrm{Sp}^\sigma(R), E) \simeq E(R)$ . This defines a morphism  $\phi': \mathcal{L}F \rightarrow E$  such that  $\phi = \phi'\iota_F$ .

It remains to show that  $\tilde{F}$  is a sheaf. But let us first show that  $\iota_{\mathcal{L}F}: (\mathcal{L}F)(R) \rightarrow (\mathcal{L}(\mathcal{L}F))(R)$  is injective for every  $k$ - $\sigma$ -algebra  $R$ . So we have to show that if  $\mu, \eta: \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$  are two morphisms having the same restriction to a fat subfunctor  $D \subset \mathrm{Sp}^\sigma(R)$ , then  $\mu = \eta$ . Let  $\hat{\mu}, \hat{\eta} \in (\mathcal{L}F)(R)$  correspond to  $\mu$  and  $\eta$  under the bijection  $(\mathcal{L}F)(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), \mathcal{L}F)$ . Replacing  $D$  by a smaller fat subfunctor of  $\mathrm{Sp}^\sigma(R)$  if necessary, we can assume that  $\hat{\mu} = (D, \mu')$  and  $\hat{\eta} = (D, \eta')$ . As in (20), we have  $\iota_F \mu' = \mu|_D$  and  $\iota_F \eta' = \eta|_D$ . By Lemma 11.6, there exists an  $R$ -covering family  $(R_i)_{i \in I}$  such that  $\mathrm{Im}(\mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)) \subset D$  for all  $i \in I$ . For  $i \in I$  let  $\mu_i: \mathrm{Sp}^\sigma(R_i) \rightarrow D \xrightarrow{\mu'} F$  and  $\eta_i: \mathrm{Sp}^\sigma(R_i) \rightarrow D \xrightarrow{\eta'} F$  be the induced morphisms. Then  $\iota_F \mu_i = \iota_F \eta_i$ . Considering the image of  $\mathrm{id}_{R_i} \in \mathrm{Sp}^\sigma(R_i)(R_i)$  in  $(\mathcal{L}F)(R_i)$  under  $\iota_F \mu_i = \iota_F \eta_i$ , shows that there exists a fat subfunctor  $D_i$  of  $\mathrm{Sp}^\sigma(R_i)$  such that  $\mu_i|_{D_i} = \eta_i|_{D_i}$ . By Lemma 11.6, there exists for every  $i \in I$  and  $R_i$ -covering family  $(S_{ij})_{j \in J_i}$  such that  $\mathrm{Im}(\mathrm{Sp}^\sigma(S_{ij}) \rightarrow \mathrm{Sp}^\sigma(R_i)) \subset D_i$  for all  $j \in J_i$ . The family  $(S_{ij})_{i \in I, j \in J_i}$  is  $R$ -covering and therefore the union  $D'$  of all  $\mathrm{Im}(\mathrm{Sp}^\sigma(S_{ij}) \rightarrow R)$  is a fat subfunctor of  $\mathrm{Sp}^\sigma(R)$  by Lemma 11.6.

$$\begin{array}{ccccccc} \mathrm{Sp}^\sigma(S_{ij}) & \longrightarrow & D_i & \hookrightarrow & \mathrm{Sp}^\sigma(R_i) & \longrightarrow & D \hookrightarrow \mathrm{Sp}^\sigma(R) \\ & & & & \searrow \eta_i \mu' & \downarrow \eta' & \downarrow \mu \\ & & & & \mu_i & \downarrow \iota_F & \downarrow \eta \\ & & & & & F & \xrightarrow{\iota_F} \mathcal{L}F \end{array}$$

Since  $\mu_i$  and  $\eta_i$  agree on  $D_i$  we see that  $\mu'$  and  $\eta'$  agree on  $D'$ . Therefore  $\hat{\mu} = \hat{\eta}$  and consequently  $\mu = \eta$  as claimed.

To show that  $\tilde{F}$  is a sheaf, it thus suffices to show that  $\mathcal{L}F$  is a sheaf whenever  $\iota_F: F(R) \rightarrow (\mathcal{L}F)(R)$  is injective for every  $k$ - $\sigma$ -algebra  $R$ . Let us identify  $F$  with a subfunctor of  $\mathcal{L}F$  via  $\iota_F$  and let  $(D, \alpha) \in (\mathcal{L}F)(R)$ . Since  $D$  is fat in  $\mathrm{Sp}^\sigma(R)$ , by Lemma 11.6, there exists an  $R$ -covering family  $(R_i)_{i \in I}$  such that  $\mathrm{Im}(\mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)) \subset D$ . Let  $\phi_i: \mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)$  denote the canonical map. The commutativity of

$$\begin{array}{ccc} \phi_i^{-1}(D) & \hookrightarrow & \mathrm{Sp}^\sigma(R_i) \\ \downarrow & \nearrow & \downarrow \phi_i \\ D & \hookrightarrow & \mathrm{Sp}^\sigma(R_i) \\ \downarrow \alpha & & \\ F & & \end{array}$$

shows that  $(\mathcal{L}F)(R) \rightarrow (\mathcal{L}F)(R_i)$  maps  $(D, \alpha)$  into  $F(R_i) \subset (\mathcal{L}F)(R_i)$ . Thus  $F$  is fat in  $\mathcal{L}F$ .

To show that  $\mathcal{L}F$  is a sheaf, it suffices to show (Proposition 11.7) that for every  $k$ - $\sigma$ -algebra  $R$ , every morphism  $\mu: D \rightarrow \mathcal{L}F$  from a fat subfunctor  $D \subset \mathrm{Sp}^\sigma(R)$  to  $\mathcal{L}F$  has a unique extension  $\mu': \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$ . The uniqueness of  $\mu'$  follows from the assumed injectivity of  $\iota_F: F(R) \rightarrow (\mathcal{L}F)(R)$ . So it remains to prove the existence of  $\mu'$ . Since  $F \subset \mathcal{L}F$  is fat,  $\mu^{-1}(F) \subset D$  is fat. Since  $D$  is fat in  $\mathrm{Sp}^\sigma(R)$  it follows that  $\mu^{-1}(F)$  is fat in  $\mathrm{Sp}^\sigma(R)$ . Let  $\mu': \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$  correspond to the image of  $\mu: \mu^{-1}(F) \rightarrow F$  in  $(\mathcal{L}F)(R)$  under the bijection  $(\mathcal{L}F)(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), \mathcal{L}F)$ . Then  $\mu'$  is an extension of  $\mu: \mu^{-1}(F) \rightarrow F \subset \mathcal{L}F$ . It remains to show that  $\mu'$  also extends  $\mu: D \rightarrow \mathcal{L}F$ . So we have to show that  $\mu(a) = \mu'(a)$  for any  $k$ - $\sigma$ -algebra  $S$  and  $a \in D(S)$ . Let  $\hat{a}: \mathrm{Sp}^\sigma(S) \rightarrow D$  correspond to  $a$  under the bijection  $D(S) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(S), D)$ . Since  $\hat{\mu}\hat{a}$  and  $\mu'\hat{a}$  have the same restriction to  $\hat{a}^{-1}(\mu^{-1}(F)) \subset \mathrm{Sp}^\sigma(S)$  it follows from the assumed injectivity of  $\iota_F: F(S) \rightarrow (\mathcal{L}F)(S)$  that  $\hat{\mu}\hat{a} = \mu'\hat{a}$ . As  $\mu(a)$  and  $\mu'(a) \in (\mathcal{L}F)(S)$  corresponds to  $\mathrm{Sp}^\sigma(S) \xrightarrow{\hat{a}} D \xrightarrow{\mu} \mathcal{L}F$  and  $\mathrm{Sp}^\sigma(S) \xrightarrow{\hat{a}} D \xrightarrow{\mu'} \mathcal{L}F$  respectively under the bijection  $(\mathcal{L}F)(S) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(S), \mathcal{L}F)$  we find that  $\mu(a) = \mu'(a)$  as desired.  $\square$



The sheaf

$$\widetilde{F}$$

from Theorem 11.8 is called the *sheaf associated with  $F$* , or the *sheafification of  $F$* . If  $\phi: F \rightarrow E$  is a morphism of functors from  $k\text{-}\sigma\text{-Alg}$  to **Sets**, then  $F \xrightarrow{\phi} E \rightarrow \widetilde{E}$  induces a morphism  $\widetilde{\phi}: \widetilde{F} \rightarrow \widetilde{E}$ . So sheafification is a functor. Indeed, as

$$\text{Hom}(\widetilde{F}, E) \simeq \text{Hom}(F, E),$$

we see that sheafification is left adjoint to the inclusion of functors into sheaves.

**Corollary 11.9.** *Let  $D$  be a fat subfunctor of a sheaf  $F: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$ , then  $\widetilde{D} = F$ .*

*Proof.* This is clear from Proposition 11.7.  $\square$

**Lemma 11.10.** *Let  $\phi: F \rightarrow E$  be a morphism of functors from  $k\text{-}\sigma\text{-Alg}$  to **Sets** such that  $\phi_R: F(R) \rightarrow E(R)$  is injective for any  $k\text{-}\sigma\text{-algebra}$   $R$ . Then  $\widetilde{\phi}_R: \widetilde{F}(R) \rightarrow \widetilde{E}(R)$  is injective for any  $k\text{-}\sigma\text{-algebra}$   $R$ .*

*Proof.* It suffices to show that  $(\mathcal{L}F)(R) \rightarrow (\mathcal{L}E)(R)$  is injective for any  $k\text{-}\sigma\text{-algebra}$   $R$ . So let  $\alpha_1: D_1 \rightarrow F$  and  $\alpha_2: D_2 \rightarrow F$  be morphism with  $D_1, D_2$  fat subfunctors of  $\text{Sp}^\sigma(R)$  such that  $\alpha_1\phi$  and  $\alpha_2\phi$  have the same image in  $(\mathcal{L}E)(R) = \varinjlim \text{Hom}(D, E)$ . Then there exists a fat subfunctor  $D$  of  $\text{Sp}^\sigma(R)$  with  $D \subset D_1 \cap D_2$  such that the restriction of  $\alpha_1\phi$  and  $\alpha_2\phi$  to  $D$  are equal. It follows from the injectivity of  $\phi$  that  $\alpha_1$  and  $\alpha_2$  have the same restriction to  $D$ .  $\square$

For simplicity, let us call a functor  $G: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Groups}$  a *group functor*. Equivalently, a group functor is a group object in the category of functors from  $k\text{-}\sigma\text{-Alg}$  to **Sets**. If  $G$  is a group functor, then the associated sheaf  $\widetilde{G}$  is naturally a group functor such that the associated morphism of functors  $\iota: G \rightarrow \widetilde{G}$  is a morphism of group functors, i.e., is compatible with the group structure. Indeed, if  $G$  is a group functor, then  $\text{Hom}(D, G)$  has naturally the structure of a group for any functor  $D: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$ . If  $R$  is a  $k\text{-}\sigma\text{-algebra}$  and  $D_1 \subset D_2$  are fat subfunctors of  $\text{Sp}^\sigma(R)$  then  $\text{Hom}(D_2, G) \rightarrow \text{Hom}(D_1, G)$  is a morphism of groups and we have an induced group structure on the limit  $(\mathcal{L}G)(R) = \varinjlim \text{Hom}(D, G)$ . This group structure is functorial in  $R$  and  $\iota_G: G \rightarrow \mathcal{L}G$  is a morphism of group functors. Applying this construction twice, yields the required group structure on  $\widetilde{G} = \mathcal{L}(\mathcal{L}G)$ . Alternatively, the group structure on  $\widetilde{G}$ , can be obtained by applying  $\widetilde{(\quad)}$  to the multiplication  $G \times G \rightarrow G$  and using the canonical isomorphism  $\widetilde{G \times G} \simeq \widetilde{G} \times \widetilde{G}$ .

If  $G$  is a group functor and  $N$  a normal subgroup functor, i.e.,  $N(R)$  is a normal subgroup of  $G(R)$  for any  $k\text{-}\sigma\text{-algebra}$   $R$ , we can define a group functor

$$G//N$$

by  $R \rightsquigarrow G(R)/N(R)$ . The crux with this functor is that it may not be a sheaf (or  $\sigma\text{-variety}$ ) if  $G$  and  $N$  are sheaves (or  $\sigma\text{-varieties}$ ). We therefore need to sheafify  $G//N$ . Sheafification is compatible with quotients in the following sense:

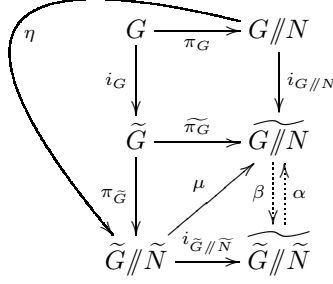
**Lemma 11.11.** *Let  $G$  be a group functor and  $N$  a normal subgroup functor. Then  $\widetilde{N}$  is a normal subgroup functor of  $\widetilde{G}$  and*

$$\widetilde{\widetilde{G//N}} \simeq \widetilde{G//N}.$$

*Proof.* By Lemma 11.10 the map  $\widetilde{N}(R) \rightarrow \widetilde{G}(R)$  is injective for any  $k\text{-}\sigma\text{-algebra}$   $R$ . Since  $N$  is normal in  $G$ ,  $\text{Hom}(D, N)$  is normal in  $\text{Hom}(D, G)$  for every fat subfunctor  $D$  of  $\text{Sp}^\sigma(R)$ . It follows that  $(\mathcal{L}N)(R)$  is normal in  $(\mathcal{L}G)(R)$  and therefore  $\widetilde{N}$  is normal in  $\widetilde{G}$ .

Since the morphism  $N \rightarrow G \rightarrow G//N$  factors through the sheaf  $E$  that maps every  $k\text{-}\sigma\text{-algebra}$  to a set with one element. Also  $\widetilde{N} \rightarrow \widetilde{G} \rightarrow \widetilde{G//N}$  factors through  $E$ . So  $\widetilde{N}$  maps into the kernel of  $\widetilde{G} \rightarrow \widetilde{G//N}$  and we obtain a morphism  $\mu: \widetilde{G//N} \rightarrow \widetilde{G//N}$ . Since  $N$  lies in the kernel of  $G \rightarrow \widetilde{G} \rightarrow \widetilde{G//N}$  we obtain a morphism  $\eta: G//N \rightarrow \widetilde{G//N}$ .

All the subdiagrams of



consisting only of solid arrows commute. By the universal property of  $i_{\tilde{G} // \tilde{N}}$  there exists a morphism  $\alpha: \widetilde{G // N} \rightarrow \widetilde{G // N}$  such that  $\alpha i_{\tilde{G} // \tilde{N}} = \mu$ . By the universal property of  $i_{G // N}$  there exists a morphism  $\beta: \widetilde{G // N} \rightarrow \widetilde{G // N}$  such that  $\beta i_{G // N} = i_{\tilde{G} // \tilde{N}} \eta$ . We will show that  $\alpha$  and  $\beta$  are inverse to each other. We have

$$\beta \pi_G i_G = \beta i_{G // N} \pi_G = i_{\tilde{G} // \tilde{N}} \eta \pi_G = i_{\tilde{G} // \tilde{N}} \pi_{\tilde{G}} i_G.$$

Therefore  $\beta \pi_G = i_{\tilde{G} // \tilde{N}} \pi_{\tilde{G}}$ . Since, for any  $k$ - $\sigma$ -algebra  $R$  and element from  $(\tilde{G} // \tilde{N})(R)$  lifts to an element of  $\tilde{G}(R)$ , this implies that  $\beta \mu = i_{\tilde{G} // \tilde{N}}$ . From  $\alpha i_{\tilde{G} // \tilde{N}} = \mu$  and  $\beta \mu = i_{\tilde{G} // \tilde{N}}$  we deduce that  $\beta \alpha i_{\tilde{G} // \tilde{N}} = i_{\tilde{G} // \tilde{N}}$ . Thus  $\beta \alpha$  is the identity on  $\widetilde{G // N}$ .

We have  $\alpha i_{\tilde{G} // \tilde{N}} \eta = \mu \eta = i_{G // N}$ . Together with  $i_{\tilde{G} // \tilde{N}} \eta = \beta i_{G // N}$ , this implies  $\alpha \beta i_{\tilde{G} // \tilde{N}} = i_{\tilde{G} // \tilde{N}}$ . Therefore  $\alpha \beta$  is the identity on  $\widetilde{G // N}$ .  $\square$

**Theorem 11.12.** *Let  $G$  be a  $\sigma$ -algebraic group and  $N \trianglelefteq G$  a  $\sigma$ -closed subgroup. Then  $G // N$  is a fat subfunctor of  $G/N$ . In particular,*

$$\widetilde{G // N} = G/N.$$

*Proof.* By Theorem 7.3 the kernel of  $G \rightarrow G/N$  equals  $N$ , i.e., for every  $k$ - $\sigma$ -algebra  $R$  the kernel of  $G(R) \rightarrow (G/N)(R)$  is  $N(R)$ . Thus the canonical map  $G(R)/N(R) \rightarrow (G/N)(R)$  is injective. Therefore we can identify  $G // N$  with a subfunctor of  $G/N$ . It follows from Lemma 7.5 that  $G // N$  is fat in  $G/N$ .  $\square$

## 11.2 The isomorphism theorems

The following theorem is the analog of the first isomorphism theorem for groups.

**Theorem 11.13.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups. Then  $\phi(G)$  is a  $\sigma$ -closed subgroup of  $H$  and the induced morphism  $G/\ker(\phi) \rightarrow \phi(G)$  is an isomorphism.*

*Proof.* We already observed in Lemma 8.4 that  $\phi(G)$  is a  $\sigma$ -closed subgroup. Since  $\ker(\phi)$  is the kernel of  $G \rightarrow \phi(G)$ , the induced morphism  $G/\ker(\phi) \rightarrow \phi(G)$  is a  $\sigma$ -closed embedding by Corollary 7.4 and so we can identify  $G/\ker(\phi)$  with a  $\sigma$ -closed  $\sigma$ -subvariety of  $G$ . Since  $\phi$  factors through  $G/\ker(\phi)$  it follows from the definition of  $\phi(G)$  that  $G/\ker(\phi) = \phi(G)$ .  $\square$

**Corollary 11.14.** *Let  $\phi: G \rightarrow H$  be a morphism of  $\sigma$ -algebraic groups. Then*

$$\phi(G) = \widetilde{\text{Im}(\phi)}.$$

*Proof.* The isomorphism  $G/\ker(\phi) \simeq \phi(G)$  identifies  $G // \ker(\phi)$  with  $\text{Im}(\phi)$ . Therefore the claim follows from Theorem 11.12.  $\square$

Let  $N$  and  $H$  be  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G$  such that  $H$  normalizes  $N$ , i.e.,  $H(R)$  normalizes  $N(R)$  for any  $k$ - $\sigma$ -algebra  $R$ . Then we can form the semidirect product  $N \rtimes H$ : This is a  $\sigma$ -algebraic group with underlying  $\sigma$ -variety  $N \times H$  and multiplication given by  $((n_1, h_1), (n_2, h_2)) \mapsto (n_1 h_1 n_2 h_1^{-1}, h_1 h_2)$  for any  $k$ - $\sigma$ -algebra  $R$  and  $n_1, n_2 \in N(R)$ ,  $h_1, h_2 \in H(R)$ . The map

$$m: N \rtimes H \rightarrow G, (n, h) \mapsto nh$$

for any  $k$ - $\sigma$ -algebra  $R$  and  $n \in N(R)$ ,  $h \in H(R)$  is a morphism of  $\sigma$ -algebraic groups. We define

$$HN := NH := m(N \rtimes H).$$

By construction  $HN$  is a  $\sigma$ -closed subgroup of  $G$  (Lemma 8.4). In fact,  $HN$  is the smallest  $\sigma$ -closed subgroup of  $G$  which contains  $N$  and  $H$ . It follows from Corollary 11.14 that  $HN$  is the sheaf associated to the functor  $R \mapsto N(R)H(R)$ . Moreover, by Lemma 8.11 we have

$$(NH)(R) = \{g \in G(R) \mid \exists \text{ faithfully flat } R\text{-}\sigma\text{-algebra } S \text{ such that } g \in N(S)H(S)\}$$

for any  $k$ - $\sigma$ -algebra  $R$ . It follows from Lemma 8.12 that  $N = m(N)$  is normal in  $HN$ .

The following theorem is the analog of the second isomorphism theorem for groups.

**Theorem 11.15.** *Let  $H$  and  $N$  be  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G$  such that  $H$  normalizes  $N$ . Then the canonical morphism*

$$H/(H \cap N) \rightarrow HN/N$$

*is an isomorphism.*

*Proof.* For every  $k$ - $\sigma$ -algebra  $R$  we have an isomorphism

$$H(R)/(H(R) \cap N(R)) \rightarrow H(R)N(R)/N(R)$$

which is functorial in  $R$ . Passing to the associated sheaves and using Lemma 11.11 we find the required isomorphism.  $\square$

The following theorem is the analog of the third isomorphism theorem for groups.

**Theorem 11.16.** *Let  $G$  be a  $\sigma$ -algebraic group,  $N \trianglelefteq G$  a normal  $\sigma$ -closed subgroup and  $\pi: G \rightarrow G/N$  the quotient. The map  $H \mapsto \pi(H) = H/N$  defines a bijection between the  $\sigma$ -closed subgroups  $H$  of  $G$  containing  $N$  and the  $\sigma$ -closed subgroups  $H'$  of  $G/N$ . The inverse map is  $H' \mapsto \pi^{-1}(H')$ . A  $\sigma$ -closed subgroup  $H$  of  $G$  containing  $N$  is normal in  $G$  if and only if  $H/N$  is normal in  $G/N$ , in which case the canonical morphism*

$$G/H \rightarrow (G/N)/(H/N)$$

*is an isomorphism.*

*Proof.* By Theorem 11.13 and Theorem 7.3 we have  $\pi(H) = H/N$ . Let us show that  $\pi^{-1}(\pi(H)) = H$  for every  $\sigma$ -closed subgroup  $H$  of  $G$  containing  $N$ . Let  $R$  be a  $k$ - $\sigma$ -algebra and  $g \in \pi^{-1}(\pi(H))(R)$ , i.e.,  $\pi(g) \in \pi(H)(R)$ . By Lemma 8.11 there exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $h \in H(S)$  with  $\pi(h) = \pi(g) \in (G/N)(S)$ . As  $\ker(\pi) = N$  by Theorem 7.3, this implies that  $gh^{-1} \in N(S) \leq H(S)$ . Therefore  $g \in H(S)$  and  $g \in H(S) \cap G(R) = H(R)$  by Lemma 8.10. Thus  $\pi^{-1}(\pi(H)) \subset H$ . The reverse inclusion is obvious.

Let us next show that  $\pi(\pi^{-1}(H')) = H'$  for a  $\sigma$ -closed subgroup  $H'$  of  $G/N$ . As  $\pi$  maps  $\pi^{-1}(H')$  into  $H'$ , it is clear from the definition of  $\pi(\pi^{-1}(H'))$  (Lemma 1.5) that  $\pi(\pi^{-1}(H')) \subset H'$ .

Let  $R$  be a  $k$ - $\sigma$ -algebra and  $h' \in H'(R)$ . There exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $g \in G(S)$  such that  $\pi(g) = h'$ . So  $g \in \pi^{-1}(H')(S)$  and  $h' = \pi(g) \in \pi(\pi^{-1}(H')(S)) \subset \pi(\pi^{-1}(H'))(S)$ . Thus  $h' \in \pi(\pi^{-1}(H'))(S) \cap H'(R) = \pi(\pi^{-1}(H'))(R)$ . Hence  $\pi(\pi^{-1}(H')) = H'$ .

If  $H$  is normal in  $G$ , then  $\pi(H)$  is normal in  $G/N$  by Lemma 8.12. Clearly  $\pi^{-1}(H')$  is normal if  $H'$  is normal.

For every  $k$ - $\sigma$ -algebra  $R$  we have an isomorphism

$$G(R)/H(R) \rightarrow (G(R)/N(R))/(H(R)/N(R)).$$

Passing to the associated sheaves and using Lemma 11.11 we obtain the required isomorphism.  $\square$

## 12 Jordan–Hölder theorem

In this section we apply the results from the previous sections to prove a Jordan–Hölder type theorem for  $\sigma$ -algebraic groups. A Jordan–Hölder type theorem for algebraic groups can be found in [Ros56], while a Jordan–Hölder type theorem for differential algebraic groups has been proved in [CS11]. As we will show, the Schreier refinement theorem also holds for  $\sigma$ -algebraic groups (Theorem 12.5). So any two decomposition series of a  $\sigma$ -algebraic group have equivalent refinements. However, a  $\sigma$ -algebraic group rarely has a decomposition series. It is therefore useful to consider more general subnormal series. The basic idea is to consider  $\sigma$ -algebraic groups up to quotients by zero  $\sigma$ -dimensional normal subgroups. Formally this is realized by replacing in the uniqueness statement of the classical Jordan–Hölder theorem the notion of isomorphism by the notion of isogeny.

Our first aim is to prove the analog of the Schreier refinement theorem. We follow along the lines of the well-known proof via the Butterfly lemma. (Cf. [Lan02, Section 1.3] and [Mil12, Chapter IX, Section 6].) We will need two analogs of elementary statements about groups.

**Lemma 12.1.** *Let  $N$ ,  $G$  and  $H$  be  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G'$  such that  $N \trianglelefteq G$  and  $N$  normalizes  $H$ . Then  $G \cap NH = N(G \cap H)$ .*

*Proof.* As  $N \leq G \cap NH$  and  $G \cap H \leq G \cap NH$  it is clear that  $N(G \cap H) \subset G \cap NH$ .

Conversely, let  $R$  be a  $k$ - $\sigma$ -algebra and  $g \in (G \cap NH)(R)$ . There exists a faithfully flat  $R$ - $\sigma$ -algebra  $S$  and  $n \in N(S)$ ,  $h \in H(S)$  such that  $g = nh$  in  $G'(S)$ . But then  $h = n^{-1}g \in G(S)$  and therefore  $g = nh \in N(S)(G(S) \cap H(S)) \subset (N(G \cap H))(S)$ . It follows from Lemma 8.10 that  $g \in (N(G \cap H))(R)$ .  $\square$

**Lemma 12.2.** *Let  $H_1 \trianglelefteq H_2$  be  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G$ . Assume that  $H_2$  normalizes  $N \leq G$ . Then  $NH_1 \trianglelefteq NH_2$ .*

*Proof.* Clearly  $N \rtimes H_1$  is a normal  $\sigma$ -closed subgroup of  $N \rtimes H_2$ . Therefore  $NH_1 = m(N \rtimes H_1)$  is a normal  $\sigma$ -closed subgroup of  $NH_2 = m(N \rtimes H_2)$  by Lemma 8.12.  $\square$

The following lemma is the analog of the Butterfly (or Zassenhaus) lemma.

**Lemma 12.3.** *Let  $N_1 \trianglelefteq H_1$  and  $N_2 \trianglelefteq H_2$  be  $\sigma$ -closed subgroups of a  $\sigma$ -algebraic group  $G$ . Then  $N_1(H_1 \cap N_2) \trianglelefteq N_1(H_1 \cap H_2)$ ,  $N_2(N_1 \cap H_2) \trianglelefteq N_2(H_1 \cap H_2)$  and*

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}.$$

*Proof.* Since  $H_1 \cap N_2$  is normal in  $H_1 \cap H_2$  it follows from Lemma 12.2 that  $N_1(H_1 \cap N_2)$  is normal in  $N_1(H_1 \cap H_2)$ . Similarly,  $N_2(N_1 \cap H_2) \trianglelefteq N_2(H_1 \cap H_2)$ . As  $H_1 \cap H_2$  normalizes  $N_1(H_1 \cap N_2)$  it follows from Theorem 11.15 that

$$\frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)} \simeq \frac{(H_1 \cap H_2)N_1(H_1 \cap N_2)}{N_1(H_1 \cap N_2)}. \quad (21)$$

Lemma 12.1 with  $N = H_1 \cap N_2$ ,  $G = H_1 \cap H_2$  and  $H = N_1$  shows that

$$(H_1 \cap H_2) \cap N_1(H_1 \cap N_2) = (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) = (H_1 \cap N_2)(N_1 \cap H_2).$$

Because  $H_1 \cap N_2 \subset H_1 \cap H_2$  we find  $(H_1 \cap H_2)N_1(H_1 \cap N_2) = N_1(H_1 \cap H_2)$ . Therefore (21) becomes

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)}.$$

By symmetry

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}.$$

$\square$

**Definition 12.4.** Let  $G$  be a  $\sigma$ -algebraic group. A subnormal series of  $G$  is a sequence

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = 1 \quad (22)$$

of  $\sigma$ -closed subgroups of  $G$  such that  $G_{i+1}$  is normal in  $G_i$  for  $i = 0, \dots, n-1$ . Another subnormal series

$$G = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_m = 1 \quad (23)$$

of  $G$  is called a refinement of (22) if  $\{G_0, \dots, G_n\} \subset \{H_1, \dots, H_m\}$ . We say that (22) and (23) are equivalent if  $n = m$  and there exists a permutation  $\pi$  such that the quotient groups  $G_i/G_{i+1}$  and  $H_{\pi(i)}/H_{\pi(i)+1}$  are isomorphic for  $i = 0, \dots, n-1$ . A subnormal series is called a decomposition series if no quotient group has a proper non-trivial normal  $\sigma$ -closed subgroup.

The following theorem is the analog of the Schreier refinement theorem.

**Theorem 12.5.** Any two subnormal series of a  $\sigma$ -algebraic group have equivalent refinements.

*Proof.* Let

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

and

$$G = H_0 \supset H_1 \supset \cdots \supset H_m = 1$$

be subnormal series of a  $\sigma$ -algebraic group  $G$ . Set  $G_{i,j} = G_{i+1}(H_j \cap G_i)$  for  $i = 0, \dots, n-1$  and  $j = 0, \dots, m$ . Then

$$G = G_0 = G_{0,0} \supset G_{0,1} \supset G_{0,2} \supset \cdots \supset G_{0,m} = G_1 = G_{1,0} \supset G_{1,1} \supset \cdots \supset G_{n-1,m} = 1$$

is a subnormal series for  $G$ . Similarly, setting  $H_{j,i} = H_{j+1}(G_i \cap H_j)$  for  $j = 0, \dots, m-1$  and  $i = 0, \dots, n$ , defines a subnormal series for  $G$ . By Lemma 12.3

$$G_{i,j}/G_{i,j+1} \simeq H_{j,i}/H_{j,i+1}.$$

□

**Corollary 12.6.** Any two decomposition series of a  $\sigma$ -algebraic group are equivalent.

*Proof.* By Theorem 12.5 there exist equivalent refinements. But a refinement of a decomposition series is necessarily trivial. □

The above corollary is not that useful as it may seem at first sight, because a  $\sigma$ -algebraic need not poses a decomposition series. Let us illustrate this with an example.

**Example 12.7.** Let  $k$  be a  $\sigma$ -field of characteristic zero. The  $\sigma$ -algebraic group  $G = \mathbb{G}_a$  does not have a decomposition series. Indeed, by [DVHW, Corollary A.3], every proper  $\sigma$ -closed subgroup  $G$  of  $\mathbb{G}_a$  is of the form  $G(R) = \{g \in R \mid f(g) = 0\}$  for some non-zero homogeneous linear difference equation  $f = \sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \cdots + \lambda_0 y$ . If  $h$  is another non-trivial linear homogeneous difference equation, then the product  $h * f$  in the sense of linear difference operators (See [Lev08, Section 3.1].) defines a  $\sigma$ -closed subgroup  $H$  of  $\mathbb{G}_a$  with  $G \subsetneq H \subsetneq \mathbb{G}_a$ . For example, for  $h = \sigma(y)$  we have

$$H(R) = \{g \in R \mid \sigma^{n+1}(g) + \sigma(\lambda_{n-1})\sigma^n(y) + \cdots + \sigma(\lambda_0)\sigma(g) = 0\}.$$

To remedy this shortcoming we need to relax the condition that the quotient groups of a decomposition series are simple.

**Definition 12.8.** A  $\sigma$ -algebraic group  $G$  with  $\sigma\text{-dim}(G) > 0$  is called almost-simple if every normal proper  $\sigma$ -closed subgroup of  $G$  has  $\sigma$ -dimension zero.

In the differential world, the almost-simple differential algebraic groups are fairly well understood. See [CS11], [Min], [Fre]. We hope to elucidate the structure of almost-simple  $\sigma$ -algebraic groups in the future. Considerable understanding of the Zariski dense  $\sigma$ -algebraic subgroups of almost-simple algebraic groups has already been obtained in [CHP02, Proposition 7.10]. See also [DVHW, Section A4].

**Example 12.9.** The  $\sigma$ -algebraic group  $G = \mathbb{G}_a$  is almost-simple. (Cf. Example 12.7.)

**Lemma 12.10.** *Let  $G$  be a  $\sigma$ -algebraic group with  $\sigma\text{-dim}(G) > 0$ . Among the  $\sigma$ -closed subgroups  $H$  of  $G$  with  $\sigma\text{-dim}(H) = \sigma\text{-dim}(G)$  there exists a unique smallest one.*

*Proof.* Let  $H_1$  and  $H_2$  be  $\sigma$ -closed subgroups of  $G$  with  $\sigma\text{-dim}(H_1) = \sigma\text{-dim}(H_2) = \sigma\text{-dim}(G)$ . By Theorem 4.6 we have  $\sigma\text{-dim}(H_1 \cap H_2) = \sigma\text{-dim}(G)$ . Thus the claim follows from Corollary 4.2.  $\square$

**Definition 12.11.** *Let  $G$  be a  $\sigma$ -algebraic group with  $\sigma\text{-dim}(G) > 0$ . The smallest  $\sigma$ -closed subgroup of  $G$  with  $\sigma$ -dimension equal to the  $\sigma$ -dimension of  $G$  is called the strong identity component of  $G$ . It is denoted by*

$$G^{so}.$$

*A  $\sigma$ -algebraic group of positive  $\sigma$ -dimension is called strongly connected if it is equal to its strong identity component.*

Thus a  $\sigma$ -algebraic group  $G$  is strongly connected if and only if it has no proper  $\sigma$ -closed subgroup with  $\sigma$ -dimension equal to the  $\sigma$ -dimension of  $G$ . It is clear from Lemma 9.18 that a strongly connected  $\sigma$ -algebraic group is connected. The strong identity component of a  $\sigma$ -algebraic group is strongly connected.

**Example 12.12.** If  $\mathcal{G}$  is a smooth connected algebraic group with  $\dim(\mathcal{G}) > 0$ , then  $G = [\sigma]_k \mathcal{G}$  is strongly connected. Indeed, as  $\mathcal{G}$  is smooth and connected  $k[\mathcal{G}[i]]$  is an integral domain for every  $i \geq 0$ . So if  $H$  is a proper  $\sigma$ -closed subgroup of  $G$ , then  $\dim(H[i]) < \dim(G[i])$  for  $i \gg 0$ . But  $\dim(G[i]) = \dim(\mathcal{G})(i+1)$  and so it follows from Theorem 3.5 that  $\sigma\text{-dim}(H) < \sigma\text{-dim}(G)$ .

The following example shows that a  $\sigma$ -integral  $\sigma$ -algebraic group need not be strongly connected.

**Example 12.13.** Let  $G$  be the  $\sigma$ -closed subgroup of  $\mathbb{G}_a^2$  given by

$$G(R) = \{(g_1, g_2) \in R^2 \mid \sigma(g_1) = g_1\} \leq \mathbb{G}_a^2(R)$$

for any  $k$ - $\sigma$ -algebra  $R$ . As  $k\{G\} = k[y_1]\{y_2\}$  with  $\sigma(y_1) = y_1$  we see that  $G$  is  $\sigma$ -integral. We have  $\sigma\text{-dim}(G) = 1$  (for example by Proposition 3.10). The  $\sigma$ -closed subgroup  $H$  of  $G$  given by  $H(R) = \{(0, g) \in R^2\}$  is isomorphic to  $\mathbb{G}_a$  and therefore also has  $\sigma$ -dimension one. It is clear from Example 12.12 that  $G^{so} = H$ .

It is obvious that  $G^{so}$  is a characteristic subgroup of  $G$  in the weak sense that for every automorphism  $\tau$  of  $G$  we have  $\tau(G^{so}) = G^{so}$ . However, the following example illustrates the somewhat disturbing fact that  $G^{so}$  need not be normal in  $G$ .

**Example 12.14.** Let  $G = N \rtimes H$  be the  $\sigma$ -algebraic group from Example 10.11. Then  $\sigma\text{-dim}(G) = 1$ . The  $\sigma$ -closed subgroup  $H = \mathbb{G}_m$  of  $G$  has  $\sigma$ -dimension one. Since  $H$  is strongly connected (Example 12.12) we see that  $H = G^{so}$ . We already noted in Example 10.11 that  $H$  is not normal in  $G$ .

**Lemma 12.15.** *Assume that  $k$  is perfect and inversive. Then a strongly connected  $\sigma$ -algebraic group is  $\sigma$ -integral.*

*Proof.* Let  $G$  be a strongly connected  $\sigma$ -algebraic group. Then  $G$  is connected and because  $\sigma\text{-dim}(G) = \sigma\text{-dim}(G_{\text{red}})$  by Lemma 10.12, we must have  $G = G_{\text{red}}$ . So  $G$  is reduced and hence integral. Similarly,  $G = G_{\sigma\text{-red}}$  by Lemma 10.12. Thus  $G$  is  $\sigma$ -integral.  $\square$

The following example shows that Lemma 12.15 fails over an arbitrary base  $\sigma$ -field. There exists a strongly connected  $\sigma$ -algebraic group which is not  $\sigma$ -reduced.

**Example 12.16.** Let  $k$  be a non-inversive  $\sigma$ -field of characteristic zero. So there exists  $\lambda \in k$  with  $\lambda \notin \sigma(k)$ . Let  $G$  be the  $\sigma$ -closed subgroup of  $\mathbb{G}_a^2$  given by

$$G(R) = \{(g_1, g_2) \in R^2 \mid \sigma(g_1) = \lambda \sigma(g_2)\}$$

for any  $k$ - $\sigma$ -algebra  $R$ . Then  $k\{G\} = k[y_1, y_2, \sigma(y_2), \dots]$  with  $\sigma(y_1) = \lambda \sigma(y_2)$ . For  $i \geq 0$  let  $G[i]$  denote the  $i$ -th order Zariski closure of  $G$  in  $\mathbb{G}_a^2$ . Then  $k[G[i]] = k[y_1, y_2, \dots, \sigma^i(y_2)]$  and therefore  $\dim(G[i]) = 1 \cdot (i+1) + 1$ , in particular  $\sigma\text{-dim}(G) = 1$ .

We claim that  $G$  is strongly connected. Suppose that  $H \leq G$  is a proper  $\sigma$ -closed subgroup with  $\sigma\text{-dim}(H) = \sigma\text{-dim}(G)$ . Let  $a_1$  and  $a_2$  denote the image of  $y_1$  and  $y_2$  in  $k\{H\}$  respectively. By [DVHW, Corollary A.3] the  $\sigma$ -ideal  $\mathbb{I}(H) \subset k\{\mathbb{G}_a^2\}$  is  $\sigma$ -generated by homogenous linear  $\sigma$ -polynomials. Thus

there exists a non-trivial  $k$ -linear relation between  $a_1, a_2, \sigma(a_2), \dots$ . If that relation would properly involve  $\sigma^i(a_2)$  for  $i \geq 1$ , then  $\sigma\text{-dim}(H) = 0$ . Thus there exists a non-trivial  $k$ -linear relation between  $a_1$  and  $a_2$ . We have  $a_1 \neq 0$  and  $a_2 \neq 0$  because otherwise  $\sigma\text{-dim}(H) = 0$ . So there exists  $\mu \in k$  with  $a_1 - \mu a_2 = 0$ . Consequently

$$0 = \sigma(a_1) - \sigma(\mu)\sigma(a_2) = \lambda\sigma(a_2) - \sigma(\mu)\sigma(a_2) = (\lambda - \sigma(\mu))\sigma(a_2).$$

Since  $\lambda \notin \sigma(k)$  this implies  $\sigma(a_2) = 0$ . But then  $\sigma\text{-dim}(H) = 0$ ; a contradiction.

Now assume that  $\lambda^2 \in \sigma(k)$ . (For example, we can choose  $k = \mathbb{C}(\sqrt{x}, \sqrt{x+1}, \dots)$  with action of  $\sigma$  determined by  $\sigma(x) = x + 1$  and  $\lambda = \sqrt{x}$ .) If  $\mu \in k$  with  $\sigma(\mu) = \lambda^2$  then  $\sigma(y_1^2 - \mu y_2^2) = 0$ . Thus  $G$  is not  $\sigma$ -reduced.

We have seen in Example 12.14 that the strong identity component need not be normal. Our next goal is to reconcile this difficulty:

**Proposition 12.17.** *Assume that  $k$  is algebraically closed and inversive. Let  $G$  be a strongly connected  $\sigma$ -algebraic group and  $H$  a normal  $\sigma$ -closed subgroup of  $G$  with  $\sigma\text{-dim}(H) > 0$ . Then  $H^{so}$  is normal in  $G$ . (In particular,  $H^{so}$  is normal in  $H$ .)*

For the proof of Proposition 12.17 we need several preparatory results.

**Lemma 12.18.** *Assume that  $k$  is algebraically closed and inversive. Let  $K$  be a  $\sigma$ -field extension of  $k$ . Then there exists a  $\sigma$ -field extension  $L$  of  $K$  such that only the elements of  $k$  are fixed by all  $\sigma$ -field automorphisms of  $L|k$ , i.e.,  $L^{\text{Aut}(L|k)} = k$ .*

*Proof.* Let us start with proving the following claim: There exists a  $\sigma$ -field extension  $L$  of  $K$  such that for all  $a \in K \setminus k$  there exists a  $\sigma$ -field automorphism  $\tau$  of  $L|k$  with  $\tau(a) \neq a$  and such that every  $\sigma$ -field automorphism of  $K|k$  extends to a  $\sigma$ -field automorphism of  $L|k$ .

Since  $k$  is algebraically closed  $K \otimes_k K$  is an integral domain. Since  $k$  is inversive  $K \otimes_k K$  is  $\sigma$ -reduced (Lemma 10.6 (ii)). Therefore the quotient field  $L$  of  $K \otimes_k K$  is naturally a  $\sigma$ -field. Consider  $L$  as a  $\sigma$ -field extension of  $K$  via the embedding  $a \mapsto a \otimes 1$ . The  $\sigma$ -field automorphism  $\tau$  of  $L|k$  determined by  $\tau(a \otimes b) = b \otimes a$  moves every element of  $K \setminus k$ . Moreover, every  $\sigma$ -field automorphism  $\tau'$  of  $K|k$  extends to  $L|k$ , for example by  $\tau'(a \otimes b) = \tau'(a) \otimes b$ .

Now let us prove the lemma. By the above claim, there exists a  $\sigma$ -field extension  $L_1|K$  such that every element of  $K \setminus k$  can be moved by a  $\sigma$ -field automorphism of  $L_1|K$  and every  $\sigma$ -field automorphism of  $K|k$  extends to a  $\sigma$ -field automorphism of  $L_1|k$ . Now apply the claim again to  $L_1|k$  to find a  $\sigma$ -field extension  $L_2|L_1$  such that every element of  $L_1 \setminus k$  can be moved by a  $\sigma$ -field automorphism of  $L_2|k$  and every  $\sigma$ -field automorphism of  $L_1|k$  extends to a  $\sigma$ -field automorphism of  $L_2|k$ . Continuing like this we obtain a chain of  $\sigma$ -field extensions  $k \subset K \subset L_1 \subset L_2 \subset \dots$ . The union  $L = \cup L_i$  has the required property.  $\square$

We need to know if the strong identity component is compatible with base extension.

**Lemma 12.19.** *Assume that  $k$  is algebraically closed and inversive. Let  $G$  be a  $\sigma$ -algebraic group with  $\sigma\text{-dim}(G) > 0$  and  $K$  a  $\sigma$ -field extension of  $k$ . Then*

$$(G_K)^{so} = (G^{so})_K.$$

*Proof.* As the  $\sigma$ -dimension is invariant under base extension (Lemma 3.11),

$$\sigma\text{-dim}((G^{so})_K) = \sigma\text{-dim}(G^{so}) = \sigma\text{-dim}(G) = \sigma\text{-dim}(G_K).$$

Therefore  $(G_K)^{so} \leq (G^{so})_K$ .

Let us now show that  $(G_K)^{so}$  descends to  $k$ , i.e., there exists a  $\sigma$ -closed subgroup  $H$  of  $G$  with  $(G_K)^{so} = H_K$ . By Lemma 12.18 there exists a  $\sigma$ -field extension  $L$  of  $K$  such that  $L^{\text{Aut}(L|k)} = k$ , where  $\text{Aut}(L|k)$  is the group of all  $\sigma$ -field automorphisms of  $L|k$ . The group  $\text{Aut}(L|k)$  acts on  $L\{G_L\} = k\{G\} \otimes_k L$  by  $k$ - $\sigma$ -algebra automorphisms via the right factor. Let  $H'$  be a  $\sigma$ -closed subgroup of  $G_L$ . Since the Hopf algebra structure maps commute with the  $\text{Aut}(L|k)$ -action,  $\tau(\mathbb{I}(H'))$  is a  $\sigma$ -Hopf ideal of  $k\{G\} \otimes_k L$  for every  $\tau \in \text{Aut}(L|k)$ . Moreover, the  $\sigma$ -dimension of the  $\sigma$ -closed subgroup of  $G_L$  defined by  $\tau(\mathbb{I}(H'))$  is equal to the  $\sigma$ -dimension of  $H'$  (cf. Lemma 3.11). Since  $\mathbb{I}((G_L)^{so})$  is the unique maximal

$\sigma$ -Hopf ideal of  $k\{G\} \otimes_k L$  such that  $\sigma\text{-dim}((G_L)^{so}) = \sigma\text{-dim}(G_L)$ , we see that  $\tau(\mathbb{I}((G_L)^{so})) = \mathbb{I}((G_L)^{so})$  for every  $\tau \in \text{Aut}(L|k)$ . Let

$$\mathfrak{a} = \{f \in \mathbb{I}((G_L)^{so}) \mid \tau(f) = f \ \forall \tau \in \text{Aut}(L|k)\} = \mathbb{I}((G_L)^{so}) \cap k\{G\}.$$

Since the action of  $\text{Aut}(L|K)$  commutes with the Hopf algebra structure maps,  $\mathfrak{a}$  is  $\sigma$ -Hopf ideal of  $k\{G\}$  and therefore corresponds to a  $\sigma$ -closed subgroup  $H$  of  $k\{G\}$ . We have  $\mathfrak{a} \otimes_k L = \mathbb{I}((G_L)^{so})$ . (See [Bou90, Corollary to Proposition 6, Chapter V, §10.4, A.V.63].) So  $H_L = (G_L)^{so}$ . As  $\sigma\text{-dim}(H) = \sigma\text{-dim}((G_L)^{so}) = \sigma\text{-dim}(G_L) = \sigma\text{-dim}(G)$  we see that  $G^{so} \leq H$ , therefore  $(G^{so})_L \leq H_L = (G_L)^{so}$ . Hence also

$$((G^{so})_K)_L = (G^{so})_L \leq (G_L)^{so} \leq ((G_K)^{so})_L.$$

Thus  $(G^{so})_K \leq (G_K)^{so}$ .  $\square$

The following example shows that the formation of the strongly connected component is in general not compatible with base extension.

**Example 12.20.** Let  $G$  be the strongly connected  $\sigma$ -algebraic group from Example 12.16. Let  $K = k^*$  be the inversive closure of  $k$  (see ([Lev08, Definition 2.1.6])) and let  $\mu \in K$  with  $\sigma(\mu) = \lambda$ . Then  $G_K$  is not strongly connected since it has the  $\sigma$ -closed subgroup  $H$  of  $\sigma\text{-dim}(H) = 1 = \sigma\text{-dim}(G)$  given by

$$H(R) = \{(g_1, g_2) \in R^2 \mid g_1 = \mu g_2\}$$

for any  $k$ - $\sigma$ -algebra  $R$ . So  $(G_K)^{so}$  is properly contained in  $(G^{so})_K = G_K$ .

Now we are prepared to prove Proposition 12.17.

*Proof of Proposition 12.17.* We have to show that the morphism of  $\sigma$ -varieties

$$\phi: G \times H^{so} \rightarrow G, (g, h) \mapsto ghg^{-1}$$

maps into  $H^{so}$ . We know from Lemma 12.15 that  $H$  and  $G$  are  $\sigma$ -integral. A fortiori  $H$  and  $G$  are perfectly  $\sigma$ -reduced. Because of Lemma 10.6 (iv) also the product  $G \times H^{so}$  is perfectly  $\sigma$ -reduced. So by Lemma 10.5, it suffices to show that  $\phi_K((G \times H^{so})(K)) \subset H^{so}(K)$  for every  $\sigma$ -field extension  $K$  of  $k$ . Let  $g \in G(K)$ . Then  $g$  induces an automorphism of  $G_K$  by conjugation. Since  $H$  is normal in  $G$  we have an induced automorphism on  $H_K$ . This automorphism maps  $(H_K)^{so}$  into  $(H_K)^{so}$ . But  $(H_K)^{so} = (H^{so})_K$  by Lemma 12.19. This shows that conjugation by  $g$  maps  $H^{so}(K)$  into  $H^{so}(K)$ . Thus  $\phi_K((G \times H^{so})(K)) \subset H^{so}(K)$  as required.  $\square$

**Definition 12.21.** Let  $G$  and  $H$  be strongly connected  $\sigma$ -algebraic groups of positive  $\sigma$ -dimension. A morphism  $\phi: G \rightarrow H$  is called an isogeny if  $\phi$  is surjective and  $\sigma\text{-dim}(\ker(\phi)) = 0$ . Two strongly connected  $\sigma$ -algebraic groups  $H_1, H_2$  of positive  $\sigma$ -dimension are called isogenous if there exists a strongly connected  $\sigma$ -algebraic group  $G$  and isogenies  $G \twoheadrightarrow H_1, G \twoheadrightarrow H_2$ .

By Theorem 11.13 and Corollary 7.9 a surjective morphism  $\phi: G \twoheadrightarrow H$  is an isogeny, if and only if  $\sigma\text{-dim}(G) = \sigma\text{-dim}(H)$ . In particular, isogenous  $\sigma$ -algebraic groups have the same  $\sigma$ -dimension.

**Lemma 12.22.** The composition of two isogenies is an isogeny.

*Proof.* Clearly the composition of surjective morphisms is surjective. If  $G_1 \rightarrow G_2$  and  $G_2 \rightarrow G_3$  are isogenies, then  $\sigma\text{-dim}(G_1) = \sigma\text{-dim}(G_2)$  and  $\sigma\text{-dim}(G_2) = \sigma\text{-dim}(G_3)$ . Therefore  $\sigma\text{-dim}(G_1) = \sigma\text{-dim}(G_3)$ .  $\square$

**Lemma 12.23.** Isogeny is an equivalence relation on the set of strongly connected  $\sigma$ -algebraic groups of positive  $\sigma$ -dimension.

*Proof.* Reflexivity and symmetry are obvious. Let us prove the transitivity. So let  $\phi_1: G \twoheadrightarrow H_1, \phi_2: G \twoheadrightarrow H_2$  and  $\phi'_2: G' \twoheadrightarrow H_2, \phi'_3: G' \twoheadrightarrow H_3$  be isogenies. The morphism  $\phi_2 \times \phi'_2: G \times G' \rightarrow H_2 \times H_2$  is surjective with kernel  $\ker(\phi_2) \times \ker(\phi'_2)$ , which has  $\sigma$ -dimension zero by Lemma 3.12. The diagonal  $D \leq H_2 \times H_2$  given by  $D(R) = \{(h_2, h_2) \mid h_2 \in H_2(R)\}$  for any  $k$ - $\sigma$ -algebra  $R$  is a  $\sigma$ -closed subgroup of  $H_2 \times H_2$  isomorphic to  $H_2$ . Therefore  $G'' = ((\phi_2 \times \phi'_2)^{-1}(D))^{so}$  is a  $\sigma$ -closed subgroup of  $G \times G'$  with



$\sigma\text{-dim}(G''') = \sigma\text{-dim}(H_2)$ . Let  $\pi: G'' \rightarrow G$  and  $\pi': G'' \rightarrow G'$  denote the projections onto the first and second factor respectively. We have the following diagram

$$\begin{array}{ccccc}
 & & G'' & & \\
 & \swarrow \pi & & \searrow \pi' & \\
 G & & & & G' \\
 \swarrow \phi_1 & & \searrow \phi_2 & \swarrow \phi'_2 & \searrow \phi'_3 \\
 H_1 & & H_2 & & H_3
 \end{array}$$

We claim that  $\pi$  and  $\pi'$  are isogenies. We have  $\ker(\pi) \leq 1 \times \ker(\phi'_2)$ . Therefore  $\sigma\text{-dim}(\ker(\pi)) = 0$  and consequently

$$\sigma\text{-dim}(\pi(G'')) = \sigma\text{-dim}(G'') = \sigma\text{-dim}(H_2) = \sigma\text{-dim}(G).$$

Since  $G$  is strongly connected, this shows that  $\pi(G'') = G$ , so  $\pi$  is surjective. Hence  $\pi$  is an isogeny. Similarly, it follows that  $\pi'$  is an isogeny. The isogenies  $\phi_1\pi$  and  $\phi'_3\pi'$  (Lemma 12.22) now show that  $H_1$  and  $H_3$  are isogenous.  $\square$

**Theorem 12.24.** *Assume that  $k$  is algebraically closed and inversive. Let  $G$  be a strongly connected  $\sigma$ -algebraic group with  $\sigma\text{-dim}(G) > 0$ . Then there exists a subnormal series*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1 \quad (24)$$

*such that  $\sigma\text{-dim}(G_i) > 0$ ,  $G_i$  is strongly connected,  $\sigma\text{-dim}(G_i/G_{i+1}) > 0$  and  $G_i/G_{i+1}$  is almost-simple for  $i = 0, \dots, n-1$ . If*

$$G = H_0 \supset H_1 \supset \cdots \supset H_m = 1 \quad (25)$$

*is another such subnormal series, then  $m = n$  and there exists a permutation  $\pi$  such that  $G_i/G_{i+1}$  and  $H_{\pi(i)}/H_{\pi(i+1)}$  are isogenous for  $i = 0, \dots, n-1$ .*

*Proof.* Let us first prove the existence statement. Among all normal proper  $\sigma$ -closed subgroups of  $G$  choose one, say  $H$ , with maximal  $\sigma$ -dimension. If  $\sigma\text{-dim}(H) = 0$ ,  $G$  is almost-simple and we are done. So let us assume that  $\sigma\text{-dim}(H) > 0$ . Since  $G$  is strongly connected,  $\sigma\text{-dim}(H) < \sigma\text{-dim}(G)$ . By construction  $G/H$  is almost-simple (Theorem 11.16). Let  $G_1 = H^{so}$ . Then  $G_1$  is normal in  $G$  by Proposition 12.17 and  $\sigma\text{-dim}(G/G_1) > 0$ . Let us show that  $G/G_1$  is almost-simple. Let  $N$  be a proper normal  $\sigma$ -closed subgroup of  $G$  containing  $G_1$ . By choice of  $H$ ,  $\sigma\text{-dim}(N) \leq \sigma\text{-dim}(H)$ , but since  $\sigma\text{-dim}(H) = \sigma\text{-dim}(G_1) \leq \sigma\text{-dim}(N)$  we have  $\sigma\text{-dim}(N) = \sigma\text{-dim}(G_1)$ . So  $G/G_1$  is almost-simple (Theorem 11.16). As  $\sigma\text{-dim}(G_1) < \sigma\text{-dim}(G)$  the claim follows by induction on  $\sigma\text{-dim}(G)$ .

Now let us prove the uniqueness statement. It follows from Theorem 12.5 that (24) and (25) have equivalent refinements. Let

$$G = G_0 \supsetneq G_{0,1} \supsetneq G_{0,2} \supsetneq \cdots \supsetneq G_{0,n_0} \supsetneq G_1 \supsetneq G_{1,1} \supsetneq \cdots \supsetneq G_{1,n_1} \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = 1 \quad (26)$$

be such a refinement of (24). For  $i = 0, \dots, n-1$ , as  $G_i$  is strongly connected and  $G_i/G_{i+1}$  is almost-simple,  $\sigma\text{-dim}(G_i/G_{i,1}) = \sigma\text{-dim}(G_i/G_{i+1}) > 0$  and  $\sigma\text{-dim}(G_{i,j}/G_{i,j+1}) = 0$  for  $j = 1, \dots, n_i - 1$ , also  $\sigma\text{-dim}(G_{i,n_i}/G_{i+1}) = 0$ . The kernel of  $G_i/G_{i+1} \twoheadrightarrow G_i/G_{i,1}$  has  $\sigma$ -dimension zero, so  $G_i/G_{i+1}$  and  $G_i/G_{i,1}$  are isogenous. In summary, we find that among the quotient groups of the subnormal series (26), there are precisely  $n$  of positive  $\sigma$ -dimension, (namely  $G_i/G_{i,1}$ ,  $i = 0, \dots, n-1$ ). A similar statement applies to the equivalent refinement of (25). Therefore  $n = m$  and there is a permutation  $\pi$  such that  $G_i/G_{i+1}$  and  $H_{\pi(i)}/H_{\pi(i+1)}$  are isogenous for  $i = 0, \dots, n-1$ .  $\square$

**Remark 12.25.** *It is clear from the proof that the uniqueness statement in Theorem 12.24 is also valid without any restriction on the base  $\sigma$ -field  $k$ .*

## 13 An application to $\sigma$ -Galois theory

A Galois theory for linear differential equations depending on a discrete parameter has been developed in [DVHW14]. In this Galois theory the Galois groups are affine difference algebraic groups. In this final section we show that under the Galois correspondence the numerical invariants introduced above, namely the difference dimension, the order and the limit degree of the Galois group correspond to well-known invariants of a difference field extension.

Let us recall the basic facts from [DVHW14]. Let  $K$  be  $\delta\sigma$ -field, i.e.,  $K$  is a field of characteristic zero equipped with a derivation  $\delta: K \rightarrow K$  and an endomorphism  $\sigma: K \rightarrow K$  which commute up to a factor. Because of this commutativity requirement the field  $k = K^\delta = \{a \in K \mid \delta(a) = 0\}$  is a  $\sigma$ -field. For example,  $K$  could be  $\mathbb{C}(\alpha, x)$  with  $\delta$  the derivation with respect to  $x$  and action of  $\sigma$  given by  $\sigma(f(\alpha, x)) = f(\alpha + 1, x)$ , in which case  $k = \mathbb{C}(\alpha)$  and  $\alpha$  is “the discrete parameter”. We are interested in linear differential systems  $\delta(y) = Ay$  with  $A \in K^{n \times n}$ . A field extension  $L$  of  $K$  equipped with extensions of  $\delta$  and  $\sigma$  is called a  $\sigma$ -Picard-Vessiot extension for  $\delta(y) = Ay$  if

- (i) there exists  $Y \in \mathrm{GL}_n(L)$  with  $\delta(Y) = AY$  such that the entries of  $Y, \sigma(Y), \sigma^2(Y), \dots$  generate  $L$  as a field extension of  $K$  and
- (ii)  $L^\delta = K^\delta$ .

Such a  $\sigma$ -Picard-Vessiot extension exists under rather mild assumptions and it is in a certain sense unique. (See [DVHW14, Section 1] and [Wib12, Section 2] for more details.)

Let  $S$  be the  $K$ -subalgebra of  $L$  generated by  $Y, \frac{1}{\det(Y)}, \sigma(Y), \frac{1}{\det(\sigma(Y))}, \dots$ . Note that  $R$  is stable under  $\delta$  and  $\sigma$ . The  $\sigma$ -Galois group  $G$  of  $L|K$  is the functor from the category of  $k$ - $\sigma$ -algebras to the category of groups, defined by associating to every  $k$ - $\sigma$ -algebra  $R$  the group  $\mathrm{Aut}(S \otimes_k R|K \otimes_k R)$  of all automorphisms of  $S \otimes_k R$  over  $K \otimes_k R$  which commute with  $\delta$  and  $\sigma$ . (The action of  $\delta$  on  $R$  is understood to be trivial.) One can show that  $G$  is a difference algebraic group ([DVHW14, Proposition 2.5]). Moreover, the choice of  $Y \in \mathrm{GL}_n(L)$  determines a  $\sigma$ -closed embedding  $G \hookrightarrow \mathrm{GL}_n$  of difference algebraic groups.

Let us also recall the definitions of the basic invariants of difference field extensions from [Lev08]. The difference transcendence degree  $\sigma\text{-trdeg}(L|K)$  of a  $\sigma$ -field extension  $L|K$  may be defined as the supremum over all non-negative integers  $n$  such that the difference polynomial ring in  $n$  difference variables over  $K$  can be embedded into  $L$ . The order  $\mathrm{ord}(L|K)$  is the transcendence degree of  $L|K$ . If there exists a finite set  $B \subset L$  such that  $B, \sigma(B), \dots$  generates  $L$  as a field extension of  $K$ , then the limit degree  $\mathrm{ld}(L|K)$  is the limit  $\lim_{i \rightarrow \infty} d_i$ , where  $d_i$  is the degree of the field extension  $K(B, \dots, \sigma^{i+1}(B))|K(B, \dots, \sigma^i(B))$ . The limit exists and does not depend on the choice of  $B$  ([Lev08, Section 4.3]). Note that the equality  $\sigma\text{-trdeg}(L|K) = \sigma\text{-dim}(G)$  has already been proved in [DVHW14] but with a different (though equivalent) definition of the difference dimension of  $G$ .

**Theorem 13.1.** *Let  $L|K$  be a  $\sigma$ -Picard-Vessiot extension with  $\sigma$ -Galois group  $G$ . Then*

$$\sigma\text{-trdeg}(L|K) = \sigma\text{-dim}(G),$$

$$\mathrm{ord}(L|K) = \mathrm{ord}(G)$$

and

$$\mathrm{ld}(L|K) = \mathrm{ld}(G).$$

*Proof.* Let  $A$  and  $Y$  be as above. For  $i \geq 0$  let  $G[i]$  denote the  $i$ -th order Zariski closure  $G$  in  $\mathrm{GL}_n$ . By Proposition 2.15 in [DVHW14] the differential field

$$L_i = K(Y, \sigma(Y), \sigma^i(Y), \frac{1}{\det(Y \dots \sigma^i(Y))}) \subset L$$

is a (standard) Picard-Vessiot extension with Galois group  $G[i]$ . Therefore  $\mathrm{trdeg}(L_i|k) = \dim(G[i])$  for all  $i \geq 0$  ([vdPS03, Corollary 1.30]). By [Lev08, Theorem 4.1.17] there exists a non-negative integer  $e$  such that  $\mathrm{trdeg}(L_i|K) = \sigma\text{-trdeg}(L|K)(i+1) + e$  for  $i \gg 0$ . Similarly, by Theorem 3.5 we have  $\dim(G[i]) = \sigma\text{-dim}(G)(i+1) + e$ . Therefore  $\sigma\text{-trdeg}(L|K) = \sigma\text{-dim}(G)$ . The equality  $\mathrm{ord}(L|K) = \mathrm{ord}(G)$  also follows from  $\mathrm{trdeg}(L_i|k) = \dim(G[i])$ .

For  $i \geq 1$  let  $\mathcal{G}_i$  denote the kernel of the projection  $G[i] \rightarrow G[i-1]$ . Then  $\mathcal{G}_i$  is the Galois group of the Picard-Vessiot extension  $L_i|L_{i-1}$  and therefore the size of  $\mathcal{G}_i$  equals the degree of  $L_i|L_{i-1}$ . This shows that  $\mathrm{ld}(L|K) = \mathrm{ld}(G)$ .  $\square$

## References

- [Arr] Carlos E. Arreche. Computing the differential Galois group of a one-parameter family of second order linear differential equations. arXiv:1208.2226.
- [Arr13] Carlos E. Arreche. A Galois-theoretic proof of the differential transcendence of the incomplete Gamma function. *J. Algebra*, 389:119–127, 2013.
- [Bou72] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra*. Hermann, Paris, 1972. Translated from the French.
- [Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.
- [Bou02] Élisabeth Bouscaren. Théorie des modèles et conjecture de Manin-Mumford (d’après Ehud Hrushovski). *Astérisque*, (276):137–159, 2002. Séminaire Bourbaki, Vol. 1999/2000.
- [Bui92] Alexandru Buium. *Differential algebraic groups of finite dimension*, volume 1506 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.
- [Bui93] Alexandru Buium. Geometry of differential polynomial functions. I. Algebraic groups. *Amer. J. Math.*, 115(6):1385–1444, 1993.
- [Bui98] Alexandru Buium. Differential subgroups of simple algebraic groups over  $p$ -adic fields. *Amer. J. Math.*, 120(6):1277–1287, 1998.
- [Cas72] Phyllis J. Cassidy. Differential algebraic groups. *Amer. J. Math.*, 94:891–954, 1972.
- [Cas75] Phyllis Joan Cassidy. The differential rational representation algebra on a linear differential algebraic group. *J. Algebra*, 37(2):223–238, 1975.
- [Cas78] Phyllis J. Cassidy. Unipotent differential algebraic groups. In *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, volume 51 of *Astérisque*, pages 83–115. Soc. Math. France, Paris, 1978.
- [Cas89] Phyllis Joan Cassidy. The classification of the semisimple differential algebraic groups and the linear semisimple differential algebraic Lie algebras. *J. Algebra*, 121(1):169–238, 1989.
- [CH] Zoé Chatzidakis and Ehud Hrushovski. On subgroups of semi-abelian varieties defined by difference equations. arXiv:1112.0920.
- [CH99] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.
- [Cha97] Zoé Chatzidakis. Groups definable in ACFA. In *Algebraic model theory (Toronto, ON, 1996)*, volume 496 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 25–52. Kluwer Acad. Publ., Dordrecht, 1997.
- [Cha01] Zoé Chatzidakis. Difference fields: model theory and applications to number theory. In *European Congress of Mathematics, Vol. I (Barcelona, 2000)*, volume 201 of *Progr. Math.*, pages 275–287. Birkhäuser, Basel, 2001.
- [CHP02] Zoé Chatzidakis, Ehud Hrushovski, and Ya’acov Peterzil. Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics. *Proc. London Math. Soc. (3)*, 85(2):257–311, 2002.
- [Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.
- [CS07] Phyllis J. Cassidy and Michael F. Singer. Galois theory of parameterized differential equations and linear differential algebraic groups. In *Differential equations and quantum groups*, volume 9 of *IRMA Lect. Math. Theor. Phys.*, pages 113–155. Eur. Math. Soc., Zürich, 2007.

- [CS11] Phyllis J. Cassidy and Michael F. Singer. A Jordan-Hölder theorem for differential algebraic groups. *J. Algebra*, 328:190–217, 2011.
- [DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. Avec un appendice it Corps de classes local par Michiel Hazewinkel.
- [Dre14] Thomas Dreyfus. Computing the Galois group of some parameterized linear differential equation of order two. *Proc. Amer. Math. Soc.*, 142(4):1193–1207, 2014.
- [DV12] Lucia Di Vizio. Approche galoisienne de la transcendance différentielle. In *Transcendance et irrationalité*, SMF Journée Annuelle [SMF Annual Conference], pages 1–20. Société Mathématique de France, 2012. arXiv:1404.3611.
- [DVHW] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference algebraic relations among solutions of linear differential equations. arXiv:1310.1289.
- [DVHW14] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.
- [EH00] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [Fre] James Freitag. Indecomposability for differential algebraic groups. arXiv:1106.0695.
- [GA] Sergey Gorchinskiy and Ovchinnikov Alexey. Isomonodromic differential equations and differential categories. *Journal de Mathématiques Pures et Appliquées*. to appear, doi: 10.1016/j.matpur.2013.11.001, arXiv:1202.0927.
- [GGO13] Henri Gillet, Sergey Gorchinskiy, and Alexey Ovchinnikov. Parameterized Picard-Vessiot extensions and Atiyah extensions. *Adv. Math.*, 238:322–411, 2013.
- [Gro70] *Schémas en groupes. I: Propriétés générales des schémas en groupes*. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151. Springer-Verlag, Berlin, 1970.
- [Hru01] Ehud Hrushovski. The Manin-Mumford conjecture and the model theory of difference fields. *Ann. Pure Appl. Logic*, 112(1):43–115, 2001.
- [Hru04] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms, 2004. arXiv:math/0406514v1, updated version available from <http://www.ma.huji.ac.il/~ehud/>.
- [HS08] Charlotte Hardouin and Michael F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.
- [Jan87] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 131 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1987.
- [Kam13] Moshe Kamensky. Tannakian formalism over fields with operators. *Int. Math. Res. Not. IMRN*, 24:5571–5622, 2013.
- [Kol48] E. R. Kolchin. Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Ann. of Math. (2)*, 49:1–42, 1948.
- [Kol85] E. R. Kolchin. *Differential algebraic groups*, volume 114 of *Pure and Applied Mathematics*. Academic Press Inc., Orlando, FL, 1985.
- [KP00] Piotr Kowalski and Anand Pillay. Pro-algebraic and differential algebraic group structures on affine spaces. *Amer. J. Math.*, 122(1):213–221, 2000.
- [KP02] Piotr Kowalski and A. Pillay. A note on groups definable in difference fields. *Proc. Amer. Math. Soc.*, 130(1):205–212 (electronic), 2002.

- [KP07] Piotr Kowalski and Anand Pillay. On algebraic  $\sigma$ -groups. *Trans. Amer. Math. Soc.*, 359(3):1325–1337 (electronic), 2007.
- [Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [Lan08] Peter Landesman. Generalized differential Galois theory. *Trans. Amer. Math. Soc.*, 360(8):4441–4495, 2008.
- [Lev] Alexander Levin. On the ascending chain condition for mixed difference ideals. *Int. Math. Res. Not. IMRN*. to appear, doi: 10.1093/imrn/rnu021.
- [Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
- [Mac97] Angus Macintyre. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88(2-3):165–180, 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).
- [Mal10] B. Malgrange. Differential algebraic groups. In *Algebraic approach to differential equations*, pages 292–312. World Sci. Publ., Hackensack, NJ, 2010.
- [Mil12] James S. Milne. Basic theory of affine group schemes, 2012. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [Min] Andrey Minchenko. On central extensions of simple differential algebraic groups. arXiv:1401.0522.
- [MO11] Andrey Minchenko and Alexey Ovchinnikov. Zariski closures of reductive linear differential algebraic groups. *Adv. Math.*, 227(3):1195–1224, 2011.
- [MO13] Andrey Minchenko and Alexey Ovchinnikov. Extensions of differential representations of  $\mathbf{SL}_2$  and tori. *J. Inst. Math. Jussieu*, 12(1):199–224, 2013.
- [MOSa] Andrey Minchenko, Alexey Ovchinnikov, and Michael F. Singer. Reductive linear differential algebraic groups and the Galois groups of parameterized linear differential equations. *Int. Math. Res. Not. IMRN*. to appear, doi: 10.1093/imrn/rnt344.
- [MOSb] Andrey Minchenko, Alexey Ovchinnikov, and Michael F. Singer. Unipotent differential algebraic groups as parameterized differential Galois groups. *J. Inst. Math. Jussieu*. to appear, doi: 10.1017/S1474748013000200.
- [MS11] Rahim Moosa and Thomas Scanlon. Generalized Hasse-Schmidt varieties and their jet spaces. *Proc. Lond. Math. Soc. (3)*, 103(2):197–234, 2011.
- [Ovc08] Alexey Ovchinnikov. Tannakian approach to linear differential algebraic groups. *Transform. Groups*, 13(2):413–446, 2008.
- [Ovc09] Alexey Ovchinnikov. Tannakian categories, linear differential algebraic groups, and parametrized linear differential equations. *Transform. Groups*, 14(1):195–223, 2009.
- [OWa] Alexey Ovchinnikov and Michael Wibmer.  $\sigma$ -Galois theory of linear difference equations. *Int. Math. Res. Not. IMRN*. to appear, doi: 10.1093/imrn/rnu060.
- [OWb] Alexey Ovchinnikov and Michael Wibmer. Tannakian categories with semigroup actions. arXiv:1403.3850.
- [Pil97] Anand Pillay. Some foundational questions concerning differential algebraic groups. *Pacific J. Math.*, 179(1):179–200, 1997.
- [Pil98] Anand Pillay. Differential Galois theory. I. *Illinois J. Math.*, 42(4):678–699, 1998.
- [Ros56] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. Math.*, 78:401–443, 1956.

- [RR39] J. F. Ritt and H. W. Raudenbush, Jr. Ideal theory and algebraic difference equations. *Trans. Amer. Math. Soc.*, 46:445–452, 1939.
- [Sca05] Thomas Scanlon. A positive characteristic Manin-Mumford theorem. *Compos. Math.*, 141(6):1351–1364, 2005.
- [Sca06] Thomas Scanlon. Local André-Oort conjecture for the universal abelian variety. *Invent. Math.*, 163(1):191–211, 2006.
- [Sit74] William Yu Sit. Typical differential dimension of the intersection of linear differential algebraic groups. *J. Algebra*, 32(3):476–487, 1974.
- [Sit75] William Yu Sit. Differential algebraic subgroups of  $SL(2)$  and strong normality in simple extensions. *Amer. J. Math.*, 97(3):627–698, 1975.
- [Sta14] The Stacks Project Authors. Stacks Project. <http://stacks.math.columbia.edu>, 2014.
- [SV99] Thomas Scanlon and José Felipe Voloch. Difference algebraic subgroups of commutative algebraic groups over finite fields. *Manuscripta Math.*, 99(3):329–339, 1999.
- [Tak72] Mitsuhiro Takeuchi. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.*, 7:251–270, 1972.
- [Tom] Ivan Tomašić. Twisted Galois stratification. arXiv:1112.0802.
- [Tom14] Ivan Tomašić. A twisted theorem of Chebotarev. *Proc. Lond. Math. Soc.*, 108(2):291–326, 2014.
- [vdPS97] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.
- [vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.
- [Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.
- [Wib12] Michael Wibmer. A Chevalley theorem for difference equations. *Math. Ann.*, 354(4):1369–1396, 2012.